UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

DAVID HORNE, DIANE BROWN, KELLY FLOOD, THURMAN BRYAN CLARK, DEBORAH PERSON, AMANDA CHAP, TIMOTHY HUTZ, LEA SANTELLO, LISA MELEGARI, DAWN EVANS, JENNIFER GRIFFIN, WILLIAM KNUDSEN, SCOTT SROKA, DOUGLAS LAKTONEN, PATRICIA TUEL, CHRISTOPHER HUTCHISON, RANDI FREEMAN, CASSEY-JO WOOD, DONNA MOSLEY, SCOTT YOUNGSTROM, ROBERT HARRIS, WILLIAM HILL, CHRIS TINEN, KENNETH PETERSON, WALTER KIVLAN, DAVID JUNGALI, PATRICIA BUHLER, EMILY BOSAK, SEAN BOSAK, JUSTIN PELTIER, PETER MAIZITIS, JERRY NUTT, MARIE CHINANDER, RAYMOND MCCARTNEY, PATRICIA MAGGIACOMO, MICHAEL MOORE, DAVID STEUFEN, JEANNIE BAGGETT, CHERYL LAWSON, IVY MADSEN, SCOTT KINGSLAND, GEORGEANN ROBERTS, PETER DE JESUS, ZANDRA MENDOZA, and TANYA PALMER, Individually and on Behalf of All Others Similarly situated,

Plaintiffs,

vs.

EQUIFAX INC. a Delaware corporation,

Defendant.

Civil Action No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Page(s)

I. FACTUAL BACKGROUND 1

A. On September 7, 2017, Equifax's computer systems were breached. 2

B. Equifax negligently left its computer systems vulnerable to the breach. 3

C. Equifax unreasonably delayed notifying affected persons whose data had been stolen. 6

D. Equifax has a record of failing to prevent data breaches. 11

E. Equifax collects consumers' personal information. 13

F. Plaintiffs and other Class members have suffered harm as a result of the data breach. 15

II. JURISDICTION AND VENUE 18

III. PARTIES 19

1. The Plaintiffs 19

a. David Horne 19

b. Diane Brown 19

c. Kelly Flood 20

d. Thurman Bryan Clark 20

e. Deborah Person 21

f. Amanda Chap 21

g. Timothy Hutz 22

h. Lea Santello 22

i. Lisa Melegari 23

j. Dawn Evans 23

k. Jennifer Griffin 24

l. William Knudsen 24

m. Scott Sroka 25

n. Douglas Laktonen 25

o. Patricia Tuel 26
p. Christopher Hutchison 26
q. Randi Freeman 27
r. Cassey-Jo Wood 27
s. Donna Mosley 28
t. Scott Youngstrom 28
u. Robert Harris 29
v. William Hill 29
w. Chris Tinen 30
x. Kenneth Peterson 30
y. Walter Kivlan 31
z. David Jungali 32
aa. Patricia Buhler 32
bb. Emily Bosak 33
cc. Sean Bosak 33
dd. Justin Peltier 34
ee. Peter Maizitis 34
ff. Jerry Nutt 35
gg. Marie Chinander 35
hh. Raymond McCartney 36
ii. Patricia Maggiacomo 36
jj. Michael Moore 37
kk. David Steufen 37
ll. Jeannie Baggett 38
mm. Cheryl Lawson 38
nn. Ivy Madsen 39
oo. Scott Kingsland 39

pp. Georgeann Roberts 40

qq. Peter de Jesus 40

rr. Zandra Mendoza 41

ss. Tanya Palmer 41

2. The Defendant 42

IV. CLASS ALLEGATIONS 42

V. COUNTS 50

COUNT I NEGLIGENCE (BROUGHT BY ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE NATIONWIDE CLASS, OR, ALTERNATIVELY, ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE STATE SUBCLASSES) 50

COUNT II NEGLIGENCE *PER SE* (BROUGHT BY ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE NATIONWIDE CLASS, OR, ALTERNATIVELY, ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE STATE SUBCLASSES) 52

COUNT III VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT GA. CODE ANN. § 10-1-370, *ET SEQ*. (BROUGHT BY ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE NATIONWIDE CLASS) 54

COUNT IV STATE CONSUMER PROTECTION LAWS (BROUGHT BY THE STATE-RESIDENT PLAINTIFFS AND THE STATE SUBCLASSES BELOW) 58

A. Common Allegations 58

B. Alabama 61

VIOLATION OF ALABAMA CONSUMER PROTECTION ACT ALA. CODE 1975 § 18-19-1, ET SEQ. (BROUGHT BY THE ALABAMA-RESIDENT PLAINTIFF AND THE ALABAMA SUBCLASS) 61

C. Alaska 64

VIOLATION OF ALASKA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT 64

ALASKA STAT. § 45.50.531 (BROUGHT BY THE ALASKA-RESIDENT PLAINTIFF AND THE ALASKA SUBCLASS) 64

D. Arizona 67

VIOLATION OF ARIZONA CONSUMER FRAUD ACT A.R.S. § 44-1521, *ET SEQ*. (BROUGHT BY THE ARIZONA-RESIDENT PLAINTIFF AND THE ARIZONA SUBCLASS) 67

E. Arkansas 68

(BROUGHT BY THE ARKANSAS-RESIDENT PLAINTIFF AND THE ARKANSAS SUBCLASS) 68

F. California 70

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §17200, *ET SEQ.* (BROUGHT BY THE CALIFORNIA-RESIDENT PLAINTIFFS AND THE CALIFORNIA SUBCLASS) 70

G. Colorado 73

VIOLATION OF COLORADO CONSUMER PROTECTION ACT COLO. REV. STAT. § 6-1-101, *ET. SEQ.* (BROUGHT BY THE COLORADO-RESIDENT PLAINTIFF AND THE COLORADO SUBCLASS) 73

H. Connecticut 75

VIOLATION OF CONNECTICUT UNFAIR TRADE PRACTICES ACT C.G.S. § 42-110A *ET SEQ.*, (BROUGHT BY THE CONNECTICUT-RESIDENT PLAINTIFF AND THE CONNECTICUT SUBCLASS) 75

I. Florida 77

VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, FLA. STAT. § 501.201, ET SEQ., AND THE UNFAIR TRADE PRACTICES STATUTES (BROUGHT BY THE FLORIDA-RESIDENT PLAINTIFF AND THE FLORIDA SUBCLASS) 77

J. Georgia 79

VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT GA. CODE ANN. § 10-1-370, *ET SEQ.* (BROUGHT BY THE GEORGIA-RESIDENT PLAINTIFF AND THE GEORGIA SUBCLASS) ... 79

K. Hawaii 83

VIOLATION OF HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION STATUTE HAW. REV. STAT. § 480-1, *ET SEQ.* (BROUGHT BY THE HAWAII-RESIDENT PLAINTIFF AND THE HAWAII SUBCLASS) 83

L. Idaho 85

VIOLATION OF PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT IDAHO CODE § 48-601, ET SEQ 85

(BROUGHT BY THE IDAHO-RESIDENT PLAINTIFF AND THE IDAHO SUBCLASS) 85

M. Illinois 88

VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 ILCS 505/1, ET SEQ. AND 720 ILCS 295/1A 88

(BROUGHT BY THE ILLINOIS-RESIDENT PLAINTIFF AND THE ILLINOIS SUBCLASS) 88

N. Iowa 91

VIOLATIONS OF PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT IOWA CODE § 714H.1, ET SEQ. 91

(BROUGHT BY THE IOWA-RESIDENT PLAINTIFF AND THE IOWA SUBCLASS) 91

O. Kentucky 95

VIOLATION OF THE KENTUCKY CONSUMER PROTECTION ACT KY. REV. STAT. § 367.110, *ET SEQ*. (BROUGHT BY THE KENTUCKY-RESIDENT PLAINTIFF AND THE KENTUCKY SUBCLASS) 95

P. Louisiana 99

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW LA. REV. STAT. ANN. §51:1401, *ET SEQ*. 99

(BROUGHT BY THE LOUISIANA-RESIDENT PLAINTIFF AND THE LOUISIANA SUBCLASS) 99

Q. Maine 102

MAINE UNFAIR TRADE PRACTICES ACT ME. REV. STAT. TIT. 5, § 205 (BROUGHT BY THE MAINE-RESIDENT PLAINTIFF AND THE MAINE SUBCLASS) 102

MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT ME. REV. STAT. TIT. 10, § 1212, *ET. SEQ*. (BROUGHT BY THE MAINE-RESIDENT PLAINTIFF AND THE MAINE SUBCLASS) 104

R. Maryland 105

MARYLAND CONSUMER PROTECTION ACT MD CODE COMMERCIAL LAW, § 13-301, *ET. SEQ*. (BROUGHT BY THE MARYLAND-RESIDENT PLAINTIFF AND THE MARYLAND SUBCLASS) 105

S. Massachusetts 107

MASSACHUSETTS CONSUMER PROTECTION ACT MASS. GEN. LAWS ANN. CH. 93A, § 1, *ET. SEQ*. (BROUGHT BY THE MASSACHUSETTS-RESIDENT PLAINTIFF AND THE MASSACHUSETTS SUBCLASS) 107

T. Michigan 110

MICHIGAN CONSUMER PROTECTION ACT MICH. COMP. LAWS § 445.903, *ET SEQ.* 110

(BROUGHT BY THE MICHIGAN-RESIDENT PLAINTIFF AND THE MICHIGAN SUBCLASS) 110

U. Minnesota 114

MINNESOTA CONSUMER FRAUD ACT MINN. STAT. § 325F.68, ET. SEQ. AND MINN. STAT. § 8.31, ET. SEQ. (BROUGHT BY THE MINNESOTA-RESIDENT PLAINTIFF AND THE MINNESOTA SUBCLASS) 114

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT MINN. STAT. § 325D.43, *ET. SEQ.* (BROUGHT BY THE MINNESOTA-RESIDENT PLAINTIFF AND THE MINNESOTA SUBCLASS) 116

V. Missouri 118

MISSOURI MERCHANDISING PRACTICES ACT MO. REV. STAT. § 407.010, *ET SEQ.* (BROUGHT BY THE MISSOURI-RESIDENT PLAINTIFF AND THE MISSOURI SUBCLASS) 118

W. Nevada 121

NEVADA DECEPTIVE TRADE PRACTICES ACT NEV. REV. STAT. § 598.0915, *ET. SEQ.*; NEV. REV. STAT. § 41.600, *ET. SEQ.* (BROUGHT BY THE NEVADA-RESIDENT PLAINTIFF AND THE NEVADA SUBCLASS) 121

X. New Hampshire 123

(BROUGHT BY THE NEW HAMPSHIRE-RESIDENT PLAINTIFF AND THE NEW HAMPSHIRE SUBCLASS) 123

Y. New Jersey 124

NEW JERSEY CONSUMER FRAUD ACT N.J. STAT. ANN. § 56:8-1, *ET. SEQ.* (BROUGHT BY THE NEW JERSEY-RESIDENT PLAINTIFF AND THE NEW JERSEY SUBCLASS) 124

Z. New York 127

NEW YORK GENERAL BUSINESS LAW N.Y. GEN. BUS. LAW § 349, *ET. SEQ.* (BROUGHT THE NEW YORK-RESIDENT PLAINTIFF AND THE NEW YORK SUBCLASS) 127

AA. North Carolina 129

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT N.C. GEN. STAT. ANN. § 75-1.1, *ET. SEQ.* (BROUGHT BY THE NORTH CAROLINA-RESIDENT PLAINTIFF AND THE NORTH CAROLINA SUBCLASS) ... 129

BB. North Dakota 132

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT N.D. CENT. CODE § 51-10-01, *ET. SEQ.* (BROUGHT BY THE NORTH DAKOTA-RESIDENT PLAINTIFF AND THE NORTH DAKOTA SUBCLASS) 132

CC. Ohio 134

VIOLATION OF OHIO CONSUMER SALES PRACTICES ACT OHIO REV. CODE ANN. § 1345, *ET SEQ*. (BROUGHT BY THE OHIO-RESIDENT PLAINTIFF AND THE OHIO SUBCLASS) 134

DD. Oklahoma 135

OKLAHOMA CONSUMER PROTECTION ACT OKLA. STAT. ANN. TIT. 15, § 751, *ET. SEQ.* (BROUGHT BY THE OKLAHOMA-RESIDENT PLAINTIFF AND THE OKLAHOMA SUBCLASS) 135

EE. Oregon 138

OREGON UNLAWFUL TRADE PRACTICES ACT OR. REV. STAT. §§ 646.605, *ET SEQ.* 138

(BROUGHT BY THE OREGON-RESIDENT PLAINTIFF AND THE OREGON SUBCLASS) 138

FF. Pennsylvania 142

PENNSYLVANIA UNFAIR TRADE PRACTICES 73 PA CONS. STAT. ANN. § 201-1, *ET. SEQ.* (BROUGHT BY THE PENNSYLVANIA-RESIDENT PLAINTIFF AND THE PENNSYLVANIA SUBCLASS) 142

GG. Rhode Island 145

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT R.I. GEN. LAWS § 6-13.1, *ET. SEQ.* (BROUGHT BY THE RHODE ISLAND-RESIDENT PLAINTIFF AND THE RHODE ISLAND SUBCLASS) 145

HH. South Carolina 147

VIOLATIONS OF THE SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT S.C. CODE ANN. § 39-5-10, ET SEQ 147

(BROUGHT BY THE SOUTH CAROLINA-RESIDENT PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS) 147

II. South Dakota 151

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT S.D. CODIFIED LAWS § 37-24-1, *ET. SEQ.* (BROUGHT BY THE SOUTH DAKOTA-RESIDENT PLAINTIFF AND THE SOUTH DAKOTA SUBCLASS) 151

JJ. Tennessee 153

TENNESSEE CONSUMER PROTECTION ACT TENN. CODE ANN. §§ 47-18-101, *ET. SEQ.* (BROUGHT BY THE TENNESSEE-RESIDENT PLAINTIFF AND THE TENNESSEE SUBCLASS)....................................153

KK. Texas..156

TEXAS DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT TEX. BUS. & COM. CODE § 17.41, *ET. SEQ.* (BROUGHT BY THE TEXAS-RESIDENT PLAINTIFF AND THE TEXAS SUBCLASS)...156

LL. Utah 158

UTAH CONSUMER SALES PRACTICES ACT UTAH CODE ANN. § 13-11-1, ET SEQ. 158

(BROUGHT BY THE UTAH-RESIDENT PLAINTIFF AND THE UTAH SUBCLASS)...158

MM. Vermont...161

VERMONT CONSUMER FRAUD ACT VT. STAT. ANN. TIT. 9, § 2451, *ET. SEQ.* (BROUGHT BY THE VERMONT-RESIDENT PLAINTIFF AND THE VERMONT SUBCLASS) 161

NN. Virginia...164

VIRGINIA CONSUMER PROTECTION ACT VA. CODE ANN. §§ 59.1-196, *ET SEQ.* 164

(BROUGHT BY THE VIRGINIA-RESIDENT PLAINTIFF AND THE VIRGINIA SUBCLASS) 164

OO. Washington..167

WASHINGTON CONSUMER PROTECTION ACT WASH. REV. CODE § 19.86.020, *ET. SEQ.* (BROUGHT BY THE WASHINGTON-RESIDENT PLAINTIFF AND THE WASHINGTON SUBCLASS)................................167

PP. West Virginia 169

WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT W. VA. CODE § 46A-6-101, *ET. SEQ.* (BROUGHT BY THE WEST VIRGINIA-RESIDENT PLAINTIFF AND THE WEST VIRGINIA SUBCLASS) 169

QQ. Wisconsin 172

WISCONSIN DECEPTIVE TRADE PRACTICES ACT WIS. STAT. § 110.18.....172

(BROUGHT BY THE WISCONSIN-RESIDENT PLAINTIFF AND THE WISCONSIN SUBCLASS) 172

COUNT V DATA BREACH STATUTES (BROUGHT BY THE STATE-RESIDENT PLAINTIFFS AND THE STATE SUBCLASSES BELOW)....175

A. California 175

VIOLATION OF CALIFORNIA DATA BREACH ACT CAL. CIV. CODE § 1798.80, *ET SEQ*. (BROUGHT BY THE CALIFORNIA-RESIDENT PLAINTIFF AND THE CALIFORNIA SUBCLASS) 175

B. Colorado 179

COLO. REV. STAT. ANN. § 6-1-716(2), *ET*. *SEQ*. (BROUGHT BY THE COLORADO-RESIDENT PLAINTIFF AND THE COLORADO SUBCLASS) 179

C. Georgia 180

GA. CODE ANN. § 10-1-912(A), *ET*. *SEQ*. (BROUGHT BY THE GEORGIA-RESIDENT PLAINTIFF AND THE GEORGIA SUBCLASS) 180

D. Hawaii 182

HAW. REV. STAT. § 487N-2(A), *ET*. *SEQ*. (BROUGHT BY THE HAWAII-RESIDENT PLAINTIFF AND THE HAWAII SUBCLASS) 182

E. Illinois 183

VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT AND CONSUMER FRAUD ACT (ON BEHALF OF ILLINOIS-RESIDENT PLAINTIFF AND THE ILLINOIS SUBCLASS) 183

F. Iowa 185

IOWA CODE ANN. § 715C.2(1), *ET*. *SEQ*. (BROUGHT BY THE IOWA-RESIDENT PLAINTIFF AND THE IOWA SUBCLASS) 185

G. Louisiana 186

LA. REV. STAT. ANN. ANN. § 51:3074(A), *ET*. *SEQ*. (BROUGHT BY THE LOUISIANA-RESIDENT PLAINTIFF AND THE LOUISIANA SUBCLASS) 186

H. Michigan 187

MICH. COMP. LAWS ANN. § 445.72(1), *ET*. *SEQ*. (BROUGHT BY THE MICHIGAN-RESIDENT PLAINTIFF AND THE MICHIGAN SUBCLASS) 187

I. New Hampshire 188

N.H. REV. STAT. ANN. § 359-C:20(I)(A), *ET*. *SEQ*. (BROUGHT BY THE NEW HAMPSHIRE-RESIDENT PLAINTIFF AND THE NEW HAMPSHIRE SUBCLASS) 188

J. Oregon 189

OR. REV. STAT. ANN. § 646A.604(1), *ET. SEQ.* (BROUGHT BY THE OREGON-RESIDENT PLAINTIFF AND THE OREGON SUBCLASS) 189

K. South Carolina 191

S.C. CODE ANN. § 39-1-90(A), *ET. SEQ.* (BROUGHT BY THE SOUTH CAROLINA-RESIDENT PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS) 191

L. Tennessee 192

TENN. CODE ANN. § 47-18-2107(B), *ET. SEQ.* (BROUGHT BY THE TENNESSEE-RESIDENT PLAINTIFF AND THE TENNESSEE SUBCLASS) 192

M. Virginia 193

VA. CODE ANN. § 18.2-186.6(B), *ET. SEQ.* (BROUGHT BY THE VIRGINIA-RESIDENT PLAINTIFF AND THE VIRGINIA SUBCLASS) 193

N. Washington 194

WASH. REV. CODE ANN. § 19.255.010(1), *ET. SEQ.* (BROUGHT BY THE WASHINGTON-RESIDENT PLAINTIFF AND THE WASHINGTON SUBCLASS) 194

O. Wisconsin 195

WIS. STAT. ANN. § 134.98(2), *ET. SEQ.* (BROUGHT BY THE WISCONSIN-RESIDENT PLAINTIFF AND THE WISCONSIN SUBCLASS) 195

PRAYER FOR RELIEF 196

JURY TRIAL DEMANDED 197

For their complaint against the Defendant Equifax Inc. ("Equifax"), Plaintiffs allege on their own behalf and on behalf of all others similarly situated, including the Classes and State Subclasses described herein, as follows:

1. A credit reporting agency must, above all else, protect the highly sensitive personal and financial information that it collects from consumers. When a consumer's information is collected by a credit reporting agency—often without the consent or even the knowledge of the consumer—the credit reporting agency must be at the absolute forefront of data security to ensure that thieves and hackers could *never* get access to the data the agency has collected. It cannot fail to patch critical software effectively and promptly, especially when fixes are available, and even more so when exploits based on the vulnerability in that software have been widely reported. And when a data breach involving up to 143 million records of innocent consumers occurs, a credit reporting agency must *immediately and accurately* notify all those affected to prevent consumers from becoming victims of identity theft. And it must take immediate steps to mitigate the damages it has caused—not half-steps that could even lead to self-enrichment. This lawsuit stems from Equifax's abject failure to follow these simple rules.

I. FACTUAL BACKGROUND

2. Equifax is one of the big three credit reporting agencies in the U.S.[1] Founded in 1899, it is the oldest of the credit bureaus and claims to maintain information on over 800 million consumers and more than 88 million businesses worldwide. Equifax's stock is listed on the New York Stock Exchange. In its 2016

[1] Experian and TransUnion are the other two. Innovis is considered a fourth credit reporting agency.

Annual Report, Equifax claimed operating revenue totaling $3.145 billion and operating income of $818 million.[2]

A. On September 7, 2017, Equifax's computer systems were breached.

3. On September 7, 2017, Equifax first disclosed that its computer systems had been hacked. The company stated it is continuing its investigation into the scope of the breach, but it indicated that: "Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017."[3]

4. Equifax admits that: "The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[4]

5. Ironically, Equifax is an agency that scores of consumers use to guard against identity theft, a service Equifax markets and sells. Businesses pay Equifax to verify customers are who they say they are. Robert Siciliano, CEO of IDTheftSecurity.com told NBC News: "Equifax is tasked with actually protecting this information in the form of identity theft protection and here we are with almost half of the country's population being affected."[5]

---

[2] *See* https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf.

[3] *See* Equifax September 7, 2017 press release at: https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 (last accessed Sept. 8, 2017) ("Equifax Press Release").

[4] Equifax Press Release.

[5] *See* https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686 (last accessed 9/8/17).

6. As NBC News further reported: "Even if you don't think you're a customer of Equifax, there's a strong possibility they still have your data. As a credit reporting agency, Equifax gets information from credit card companies, banks, lenders and retailers to help it determine a person's credit score."[6]

B. Equifax negligently left its computer systems vulnerable to the breach.

7. The massive data breach could have been prevented and should have been detected and disclosed earlier. While Equifax admits the intrusion occurred at least as early as "mid-May" 2017, Equifax claims it was first detected on July 29, 2017. Equifax—a company whose business is the collection and storage of extremely sensitive and valuable data—thus admits its systems were compromised for ten full weeks before it had any idea it had been hacked.

8. But what makes this breach even worse is that it was fully preventable. Equifax had notice of the software vulnerability that allowed this attack on 143 million Americans' data for some *two months* before the breach occurred. In fact, there were press reports of widespread attempts by hackers to exploit this vulnerability. Yet Equifax failed to take the steps necessary to secure its treasure of consumers' personal information—or to seal off *any* outside access to this treasure while it worked on a fix--if it indeed made any effort to do so in response to notice of the vulnerability.

9. In the days following the September 7, 2017 revelation of this breach, there were reports that the breach occurred due to a vulnerability in an open-source web application framework called Apache Struts.[7] At first the surmise was that the

[6] *See id.*

[7] *E.g.*, "Apache Foundation rebuffs allegation it allowed Equifax attack," available at https://www.theregister.co.uk/2017/09/11apache_rebuts_equifax_allegation/ (last accessed Sept. 11, 2017).

vulnerability may have been one announced in early September 2017, and thus new to all.[8] But the Apache Struts Foundation questioned this report given the timing of the announcement of that vulnerability versus Equifax's disclosure that its data storage may have been breached as early as mid-May 2017 (and that it learned of this breach in late July 2017).[9]

10. And now Equifax admits that it was the *March 2017* Apache Struts bug that one or more hackers exploited. In a September 13, 2017 post to its equifaxsecurity2017.com breach-information website (an Orwellian name if there ever were one, given the reason for creation of the site), Equifax writes:

> **1) Updated information on U.S. website application vulnerability.** Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.[[10]]

11. "Apache Struts CVE-2017-5638" is a critical vulnerability that has been publicly disclosed and widely known since March 2017. In fact, the Apache Software Foundation gave public notice on March 7, 2017,[11] after making a fix freely available on March 6, 2017.[12]

---

[8] *E.g.*, *id.*

[9] *E.g.*, *id.*; *see also* "The Apache Software Foundation Blog," Sept. 9, 2017, available at https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax (last accessed Sept. 11, 2017).

[10] www.equifaxsecurity2017.com/ (last accessed Sept. 14, 2017).

[11] *See* "Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability," *Qualys Threat Protection*, Mar. 8, 2017, available at https://threatprotect.qualys.com/2017/03/08/apache-struts-jakarta-multipart-parser-remote-code-execution-vulnerability/ (last accessed Sept. 14, 2017).

[12] *See, e.g.*, "Critical vulnerability under 'massive' attack imperils high-impact sites [Updated]," *Ars Technica*, Mar. 9, 2017, available at https://arstechnica.com/information-

12. And a critical fix it was. Ars Technica reported on March 9, 2017,[13] and March 14, 2017,[14] that sites using this vulnerable software framework were under heavy attack by hackers. As Ars Technica put it, "In a string of attacks that have escalated over the past 48 hours, hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used by banks, government agencies, and large Internet companies."[15] The bug was described as "trivial to exploit" and "under attack by hackers who [we]re exploiting it to inject commands of their choice into Struts servers that have yet to install the update," per warnings from researchers.[16] "Making matters worse, at least two working exploits [were] publicly available."[17] In fact, "[e]ight days after developers patched a critical flaw in the Apache Struts Web application framework, there ha[d] been no let-up in the volley of attacks attempting to exploit the vulnerability, which affects a disproportionate number of high-impact websites," according to a security researcher.[18]

13. Yet despite the issuance of a patch, publicity about the barrage of attacks attempting to exploit the reported vulnerability, and the extremely sensitive personal and financial information[19] gathered and stored by Equifax, Equifax

---

technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/ (last accessed Sept. 14, 2017.

[13] *Id.*

[14] *See, e.g.*, "In-the-wild exploits ramp up against high-impact sites using Apache struts," *Ars Technica*, Mar. 14, 2017, available at https://arstechnica.com/information-technology/2017/03/in-the-wild-exploits-ramp-up-against-high-impact-sites-using-apache-struts/ (last accessed Sept. 14, 2017.

[15] *See* n.12, *supra*.

[16] *Id.*

[17] *Id.*

[18] *See* n.14, *supra*.

[19] Except where indicated by other specific reference or context, Plaintiffs use the term "personal and financial information" throughout this Complaint also to mean Personal Information (so-called PI) or Personally Identifiable Information (so-called PII).

neglected to take the steps necessary to neutralize the possibility of its systems getting hacked—or to do so effectively in a timely fashion.[20] The result is the massive data breach that is the subject of this complaint, with serious consequences likely to follow—perhaps for decades—for some 143 million Americans.

C. Equifax unreasonably delayed notifying affected persons whose data had been stolen.

14. Shockingly, the entirely preventable Equifax breach was not disclosed for *nearly six weeks* after Equifax's self-delayed discovery. Instead of promptly detecting and promptly notifying the hundreds of millions of consumers whose complete identity information was stolen by "criminals," Equifax said nothing, leaving consumers' data in the hands of "criminals'" unfettered for at least three months between the time the breach started and the time Equifax publically announced it. Incredibly, two days *after* Equifax admitted it detected the breach, company executives sold over $1.8 million of company stock before its collapse on September 8, 2017—when Equifax ultimately did disclose the massive breach. Equifax plainly did not take the necessary and reasonable steps to protect its data storage systems from a known and fixable vulnerability, which allowed the attack, and it absolutely failed to promptly notify affected consumers once it learned of it.

15. In an exercise of understatement to the extreme, Equifax Chairman and CEO Richard F. Smith stated:

[20] On September 15, 2017, Equifax admitted that it learned of the Apache Struts vulnerability in March 2017 but that whatever steps it took to apply the patch to its systems were ineffective. (*See* Press Release, Equifax, Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes (Sept. 15, 2017), available at https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/ (last accessed Sept. 18, 2017).) Evidently it did not successfully apply the patch until late July or early August 2017—though Plaintiffs have no actual knowledge that this later effort was any more successful than the first attempt. (*Id.*)

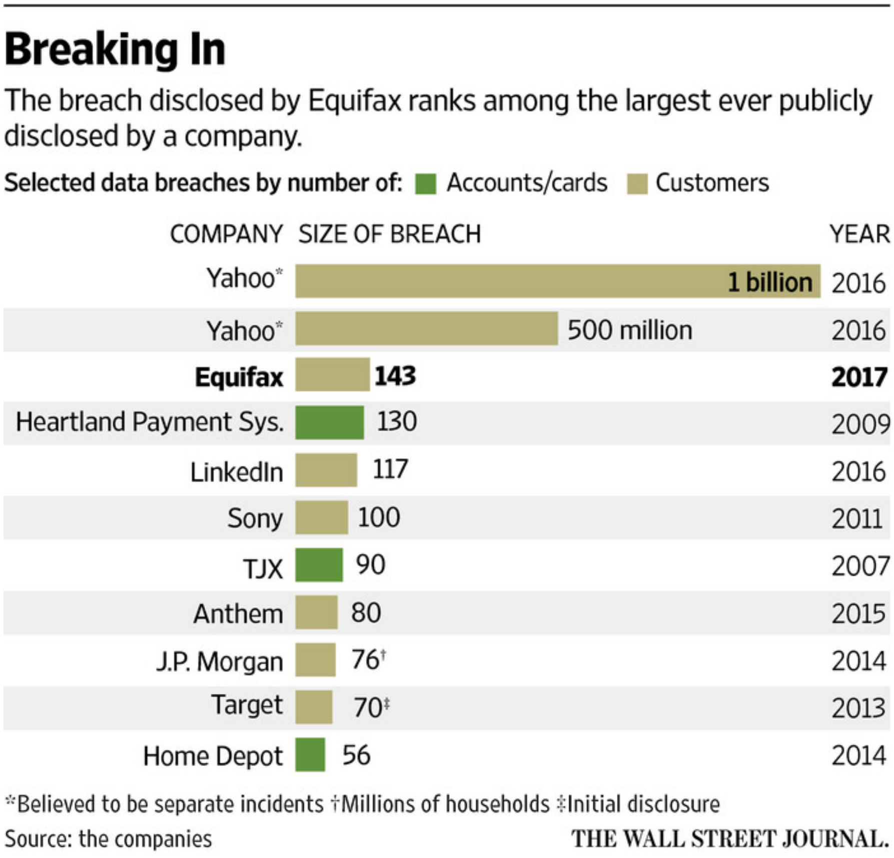
> This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes. We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations….[[21]]

16. Obviously, Equifax's "pride" in protecting data was misplaced. The massive breach of trust and Equifax's duty to safeguard sensitive data speaks for itself. Equifax did not do nearly enough to protect the consumer data that it stored and used to make its extraordinary profits. All it had to do was install a patch that was publicly known and available to it for months. And there is no possible explanation for its decision to keep this massive data breach secret for six weeks, especially while its own executives dumped stock to avoid the inevitable drop in share price.

17. The Wall Street Journal made the scope of the Equifax breach graphically clear:[22]

[21] *Id.*

[22] *Equifax Reports Data Breach Possibly Affecting 143 Million U.S. Consumers,* Wall Street Journal, Sept. 8, 2017. Viewed 9/8/17 at: https://www.wsj.com/articles/equifax-reports-data-breach-possibly-impacting-143-million-u-s-consumers-1504819765?mod=pls_whats_news_us_business_f


Breaking In
The breach disclosed by Equifax ranks among the largest ever publicly disclosed by a company.
Selected data breaches by number of: Accounts/cards Customers
COMPANY
SIZE OF BREACH
YEAR
Yahoo*
1 billion
2016
Yahoo*
500 million
2016
Equifax
143
2017
Heartland Payment Sys.
130
2009
LinkedIn
117
2016
Sony
100
2011
TJX
90
2007
Anthem
80
2015
J.P. Morgan
76†
2014
Target
70‡
2013
Home Depot
56
2014
*Believed to be separate incidents †Millions of households ‡Initial disclosure
Source: the companies
THE WALL STREET JOURNAL.

18. Alarmingly, and directly evidencing Equifax's woeful and negligent efforts at safeguarding consumers' data, the hack was not particularly sophisticated. As reported by Forbes:

> So how did hackers gain access to the Equifax data? By exploiting a vulnerability on one of the company's U.S.-based web servers. On the surface, at least, that seems to indicate that one of the three major U.S. credit bureaus was victimized by a relatively unsophisticated attack.
>
> Alex Heid, chief security researcher at SecurityScorecard has seen this before. "As surprising as it seems, the same web application vulnerabilities from decades ago are still some of the primary vectors that are leveraged by hackers in modern attack scenarios," he said in a comment to Forbes. Heid added that "it seems that the underlying legacy codebase that handled the [Equifax] web

> application was vulnerable enough for an attacker to exploit."[[23]]

19. Equifax knows that it was not doing enough to protect the sensitive information it stored. Chairman and CEO Smith admits: "Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, ***we recognize we must do more***. And we will."[24] But promises to do better in the future will not help the 143 million U.S. consumers whose complete identities have been stolen and have already, or likely will soon, flood the dark web with everything identity thieves need to destroy consumers' financial lives, wellbeing, and credit.

20. There is little doubt victims of the data breach will suffer significant and persistent financial harm as a result. "It's one of the worst hacks imaginable," said Dan Guido, CEO of the cyber-security firm Trail of Bits. "People should be extraordinarily angry at companies like Equifax. We place a huge amount of trust in them about money matters but they're so easily compromised by simplistic attacks like this one."[25]

21. And most affected consumers might never have signed up or agreed to provide their sensitive data to Equifax. Rather, as reported in Yahoo News:

> Unlike a credit card company or retailer, consumers generally don't choose to do business with credit reporting firms. Instead, credit reporting companies gather information on consumers as part of their business.
>
> "The credit bureaus collect highly sensitive consumer data, including Social Security numbers and detailed credit histories, and they have a legal and ethical

[23] *See* https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#407d92d7356f

[24] *See* Equifax Press Release.(emphasis added).

[25] *See* Allen St. John, *Equifax Data Breach: What Consumers Need to Know*, CONSUMER REPORTS (updated Sept. 21, 2017), available at https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/.

> obligation to protect it," said Jessica Rich, vice president of consumer policy and mobilization at Consumer Reports.
>
> "While it's fine that Equifax is offering consumers free credit card monitoring, that's just a Band-Aid," she added. "Companies need to take data security much more seriously so these breaches don't happen in the first place. That's why we need stronger data security laws with tougher penalties."[[26]]

22. In addition to selling Equifax consumer data to other fraudsters on the black market, the thieves could use the data to set up fraudulent financial accounts in victims' names, such as credit card accounts.

23. With access to Social Security numbers, birthdates, employment information, and income data, fraudsters could also file false tax returns, with the goal of claiming a fraudulent refund. That's a growing problem in the U.S., with the Internal Revenue Service investigating thousands of false return cases each year.

24. Alarmingly, Equifax has yet to personally notify the particular victims of the data breach, instead setting up a website that renowned security expert Brian Krebs describes as "completely broken at best, and little more than a stalling tactic or sham at worst."[27]

25. Krebs writes:

> WEB SITE WOES
>
> As noted in yesterday's breaking story on this breach, the Web site that Equifax advertised as the place where concerned Americans could go to find out whether they were impacted by this breach — equifaxsecurity2017.com — is completely broken at best, and little more than a stalling tactic or sham at worst.

---

[26] *See id.*

[27] *See* Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, KREBS ON SECURITY (Sept. 8, 2017), available at https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

> In the early hours after the breach announcement, the site was being flagged by various browsers as a phishing threat. In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones.
>
> Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring service we were eligible for was not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.[[28]]

26. All the while, the Equifax-described "criminals" have everything they need to open false credit card accounts, bank accounts, loans, and can even file false tax returns and steal refunds owed to consumers whose records have been stolen.

D. Equifax has a record of failing to prevent data breaches.

27. Earlier this very year, Equifax's computer security was breached on two separate occasions First, Equifax disclosed that its TALX payroll division was also hacked. As reported by Brian Krebs, "Identity thieves who specialize in tax refund fraud had big help this past tax year from Equifax, one of the nation's largest consumer data brokers and credit bureaus. . . . Equifax says crooks were able to reset the 4-digit PIN given to customer employees as a password and then steal W-2 tax data after successfully answering personal questions about those employees."[29]

---

[28] *See id.*

[29] *See* Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY (May 18, 2017), available at https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/

28. Equifax admitted unauthorized access to customers' employee tax records happened between April 17, 2016 and March 29, 2017.[30] For over a year Equifax's customers' employee data was being stolen—and Equifax apparently had no idea, or at least did nothing to stop it.

29. Security experts publicly told Equifax that it was not doing enough:

> Generally. Forensically. Exactly. Potentially. Actually. Lots of hand-waving from the TALX/Equifax suits. But Equifax should have known better than to rely on a simple PIN for a password, says Avivah Litan, a fraud analyst with Gartner Inc.
>
> "That's so 1990s," Litan said. "It's pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN."
> Litan said TALX should have required customers to use stronger two-factor authentication options, such as one-time tokens sent to an email address or mobile device (as Equifax now says TALX is doing — at least with those we know were notified about possible employee account abuse).[[31]]

30. Second, on September 18, 2017, Equifax disclosed a separate data breach in March 2017 that it claims was unrelated to the breach that led to its loss of account information for 143 million Americans.[32] While Equifax provided little detail of this prior data breach, it disclosed that it hired FireEye, Inc.'s Mandiant investigations group upon discovery of suspicious network activity. That investigation was apparently concluded without discovery of the vulnerability

---

[30] *See id.*

[31] *See id.*

[32] Robert McMillan & AnnaMaria Andriotis, *Equifax Discloses Earlier Cybersecurity Incident, But No* Details, THE WALL STREET JOURNAL (updated Sept. 19, 2017), available at https://www.wsj.com/articles/equifax-discloses-earlier-cybersecurity-incident-but-no-details-1505786212.

leading to the massive breach which Equifax admits began in May 2017. Equifax re-hired Mandiant in response to the massive, most recent breach.[33]

31. Quite obviously, Equifax did not learn from its mistakes. It followed its negligent protection of employee data at its TALX subsidiary, and negligent protection of its systems as evident from the March 2017 data breach, with negligent protection of the personal and financial information of nearly half the adult population of the United States. It ignored public warnings about a specific threat and public indications that the threat was being widely exploited by hackers. It had unfettered access and ample time to install a patch in an effective manner that would have entirely prevented this catastrophe for 143 million consumers. But it did not do it. As a result, "criminals" have stolen consumers names, Social Security numbers, birthdates, driver's license numbers, addresses, and in some cases credit history and credit card numbers.

E. Equifax collects consumers' personal information.

32. Equifax is one of the three major credit reporting agencies in the United States and is currently ranked 703 on the "Fortune 1000" list of top U.S. companies, with $3.145 billion in revenue.[34] Equifax markets and sells consumer information and credit history, including to creditors and prospective creditors who seek such information in the course of selling merchandise, goods, and services. Its profits are uniquely derived from the information it gathers about all consumers, whether or not such consumers have ever purchased anything from Equifax or knowingly provided information to it.

---

[33] *See id.*

[34] FORTUNE, http://fortune.com/fortune500/list/filtered?searchByName=equifax (last accessed Sept. 21, 2017).

33. Equifax is acutely aware that the consumer and business information it stores is highly sensitive and highly valuable to identity thieves and other criminals. On its website, Equifax states:

> **Privacy**
>
> For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.
>
> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax[[35]]

34. There is little question that the above policy demonstrates Equifax was well aware of the need for it to protect consumers' highly valuable personal and financial information, including Personal Identifying Information ("PII"), such as Social Security numbers and driver's license numbers.

35. While Equifax's collection of current customer and associate data may itself be legal, it cannot be questioned that by collecting and storing such extensive and detailed customer data, Equifax creates an obligation for itself to use every means available to it to protect this data from falling into the hands of criminals. This obligation would obviously include using the latest and strongest methods to prevent website application exploitation, but this is exactly the simplistic attack that led to the massive data breach in this case.

36. In addition to actually securing its data from web application exploitation, by installing publicly available and known critical patches, another

---

[35] *See* Equifax, Privacy, available at http://www.equifax.com/privacy/ (last accessed Sept. 21, 2017).

rudimentary step Equifax could have and should have taken is encryption. That is, Equifax should have converted consumers' sensitive information into coded strings that would not be immediately useful, or even identifiable to cyber-thieves. Yet Equifax apparently did not even take that step. It stored consumers' most sensitive information, including Social Security numbers, birth dates, drivers' license numbers and other credit information in plain text, readily identifiable and usable by anyone.

F. Plaintiffs and other Class members have suffered harm as a result of the data breach.

37. As a result of Equifax's unfair, inadequate, and unreasonable data security, cyber-criminals now possess the personal and financial information of Plaintiffs and the Class. Unlike credit card data breaches, like those recently at Target Corp. and Home Depot, the harm here cannot be attenuated by cancelling and reissuing credit cards. With Social Security numbers, names, addresses, birthdates, driver's license numbers, and credit information, criminals can open entirely new credit accounts and bank accounts, and garner millions through fraud that victims will not be able to detect until it is too late. Victims' credit profiles can be destroyed and they will lose the ability to legitimately borrow money, obtain credit, or even open bank accounts.

38. Further, criminals can file false federal and state tax returns in victim's names, preventing or at least delaying victims' receipt of their legitimate tax refunds and potentially making victims targets of IRS and state tax investigations. At the very least, victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, get student loans, or buy or rent furniture or a new TV, let alone complete a major purchase such as a new car or home, without taking the time to

request that the freeze be suspended, waiting the days it can take for that to occur, and then reinstating the freeze. Further, there are four major reporting agencies, so consumers may need to take these steps with all of them because they will not know which bureau a creditor may consult. Also, in many states, and in many circumstances, such freezes cost the consumer money. Evidently, Equifax will, for a short time, not charge for Equifax freezes—but it is offering no relief for the monetary cost to go through this process at the other three major credit reporting agencies, let alone for the value of time that will be spent doing all of this.

39. Immediate notice of a data breach is essential to obtain the best protection afforded by identity theft protection services. Equifax failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiffs and the Class resulting from the breach. Equifax knew its systems were compromised at least as early as July 29, 2017, yet it made no disclosures until September 7, 2017. Even then, it set up a cryptic website that collected further information, then instructed all consumers, even persons inputting bogus information, to come back later. Such delays are unwarranted, and directly increase the likelihood that thieves will be able to steal victims' identities before victims even know that they are at risk.

40. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. A credit card number trades for under $10 on the black market. Magnetic track data increases the price, and a card with full personal information

such as an address, phone number, and email address ("fullz") are traded at around $25 per record.[36]

41. But this breach is far more valuable. The data breach consists of over 143 million records that include name, address, birthdate, SSN, drivers' license numbers, employment information, and even income. Complete identity records like those at issue here can sell for up to $250-$400 on the black market, making this a breach potentially worth in excess of $500 billion to cybercriminals.[37]

42. The personal and financial information that Equifax failed to adequately protect, including Plaintiffs' identifying information and SSNs, are "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, and file false federal and state tax returns.

43. Although Equifax is offering free credit monitoring to some customers, the credit monitoring services do little to prevent wholesale identity theft. Moreover, experts warn that batches of stolen information will not be immediately dumped on the black market. "[O]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed. . .They often wait until consumers are less likely to be on the lookout for fraudulent activities."[38] In light of the seriousness of this breach and the nature of the data involved, one year of credit monitoring is decidedly not enough.

---

[36] Max Cherney, *It's Surprisingly Cheap to Buy Stolen Bank Details*, MOTHERBOARD (Dec. 23, 2013), available at https://motherboard.vice.com/en_us/article/nzewpx/its-surprisingly-cheap-to-buy-stolen-bank-details (last accessed Sept. 21, 2017).

[37] *See* http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf (last accessed Feb. 6, 2015).

[38] http://online.wsj.com/news/articles/SB10001424052702304856504579337263720948556 (last accessed Feb. 6, 2015).

44. This is especially true given the hackers' theft of SSNs, which unlike credit cards, are not reissued. A cybercriminal, especially one with millions of SSN records, can hold on to stolen information for years until the news of the theft has subsided, then steal a victim's identity, credit, and bank accounts, resulting in thousands of dollars in losses and lost time and productivity. Thus, Plaintiffs and the Class must take additional steps to protect their identities. And Plaintiffs and the Class must bear the burden and expense of identity and credit monitoring, and heightened vigilance for years to come.

II. JURISDICTION AND VENUE

45. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). At least one Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 putative class members.

46. This Court has personal jurisdiction over Equifax because Equifax has its principal place of business in, and is a resident of, Georgia, and because it regularly conducts business in Georgia and has minimum (and extensive) contacts with Georgia.

47. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax regularly conducts business and resides in this district, a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims were committed in this district, Plaintiff Dawn Evans resides in this district, and property that is the subject of the Plaintiffs' claims are in this district.

III. PARTIES

1. The Plaintiffs

a. David Horne

48. Plaintiff David Horne was an Alaska resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Horne also was a resident of Alaska on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Horne remains an Alaska resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Horne: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Horne's data was "impacted."

b. Diane Brown

49. Plaintiff Diane Brown was an Arizona resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Brown also was a resident of Arizona on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Brown remains an Arizona resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Brown: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Brown's data was "impacted."

c. Kelly Flood

50. Plaintiff Kelly Flood was an Arizona resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Flood also was a resident of Arizona on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Flood remains an Arizona resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Flood: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Flood's data was "impacted." After learning of this breach, Plaintiff Flood paid for credit freezes in the total sum of $5.00.

d. Thurman Bryan Clark

51. Plaintiff Thurman Bryan Clark was an Arkansas resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Clark also was a resident of Arkansas on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Clark remains an Arkansas resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Clark: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Clark's data was "impacted."

e. Deborah Person

52. Plaintiff Deborah Person was a California resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Person also was a resident of California on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Person remains a California resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Person: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Person's data was "impacted." After learning of this breach, Plaintiff Person paid for credit freezes at the credit bureaus, in the total sum of $20.

f. Amanda Chap

53. Plaintiff Amanda Chap was a California resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Chap also was a resident of California on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Chap remains a California resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Chap: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that

Plaintiff Chap's data was "impacted." After learning of this breach, Plaintiff Chap paid for credit freezes at the credit bureaus, in the total sum of $20.

g. Timothy Hutz

54. Plaintiff Timothy Hutz was a Colorado resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Hutz also was a resident of Colorado on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Hutz remains an Connecticut Colorado resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Hutz: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Hutz's data was "impacted."

h. Lea Santello

55. Plaintiff Lea Santello was a Connecticut resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Santello also was a resident of Connecticut on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Santello remains a Connecticut. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Santello: "Based on the information provided, we believe that your personal information may have been impacted by

this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Santello's data was "impacted."

i. Lisa Melegari

56. Plaintiff Lisa Melegari was a Florida resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Melegari also was a resident of Florida on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Melegari remains a Florida resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Melegari: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Melegari's data was "impacted."

j. Dawn Evans

57. Plaintiff Dawn Evans was a Georgia resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Evans also was a resident of Georgia on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Evans remains a Georgia resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Evans: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has

reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Evans' data was "impacted." After learning of this breach, Plaintiff Evans paid for credit freezes at the credit bureaus, in the total sum of $45.

k. Jennifer Griffin

58. Plaintiff Jennifer Griffin was a Hawaii resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Griffin also was a resident of Hawaii on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Griffin remains a Hawaii resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Griffin: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Griffin's data was "impacted." After learning of this breach, Plaintiff Griffin paid for credit freezes at the credit bureaus, in the total sum of $15.

l. William Knudsen

59. Plaintiff William Knudsen was an Idaho resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Knudsen also was a resident of Idaho on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Knudsen remains an Idaho resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at

https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Knudsen: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Knudsen's data was "impacted."

m. Scott Sroka

60. Plaintiff Scott Sroka was an Illinois resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Sroka also was a resident of Illinois on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Sroka remains an Illinois resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Sroka: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Sroka's data was "impacted."

n. Douglas Laktonen

61. Plaintiff Douglas Laktonen was an Indiana resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Laktonen also was a resident of Indiana on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Laktonen remains an Indiana resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at

https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Laktonen: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Laktonen's data was "impacted."

o. Patricia Tuel

62. Plaintiff Patricia Tuel was an Iowa resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Tuel also was a resident of Iowa on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Tuel remains an Iowa resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Tuel: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Tuel's data was "impacted."

p. Christopher Hutchison

63. Plaintiff Christopher Hutchison was a Kentucky resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Hutchison also was a resident of Kentucky on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Hutchison remains a Kentucky resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at

https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Hutchison: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Hutchison's data was "impacted."

q. Randi Freeman

64. Plaintiff Randi Freeman was a Louisiana resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Freeman also was a resident of Louisiana on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Freeman remains a Louisiana resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Freeman: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Freeman's data was "impacted."

r. Cassey-Jo Wood

65. Plaintiff Cassey-Jo Wood was a Maine resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Wood also was a resident of Maine on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Wood remains a Maine resident. Per the Defendant's advice, Plaintiff

used its “Check Potential Impact” tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant’s tool returned the following message to Plaintiff Wood: “Based on the information provided, we believe that your personal information may have been impacted by this incident.” Furthermore, because Equifax has reported that some 143 million U.S. individuals’ data was accessed via this breach, it is virtually certain that Plaintiff Wood’s data was “impacted.”

s. Donna Mosley

66. Plaintiff Donna Mosley was a Maryland resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Mosley also was a resident of Maryland on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Mosley remains a Maryland resident. Per the Defendant’s advice, Plaintiff used its “Check Potential Impact” tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant’s tool returned the following message to Plaintiff Mosley: “Based on the information provided, we believe that your personal information may have been impacted by this incident.” Furthermore, because Equifax has reported that some 143 million U.S. individuals’ data was accessed via this breach, it is virtually certain that Plaintiff Mosley’s data was “impacted.” After learning of this breach, Plaintiff Mosley paid for credit freezes at the credit bureaus, in the total sum of $10.

t. Scott Youngstrom

67. Plaintiff Scott Youngstrom was a Massachusetts resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Youngstrom also was a resident of Massachusetts on

and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Youngstrom remains a Massachusetts resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Youngstrom: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Youngstrom's data was "impacted."

u. Robert Harris

68. Plaintiff Robert Harris was a Michigan resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Harris also was a resident of Michigan on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Harris remains a Michigan resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Harris: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Harris's data was "impacted."

v. William Hill

69. Plaintiff William Hill was a Minnesota resident during the period from mid-May through July 2017, when, according to Equifax, the data breach

occurred. Plaintiff Hill also was a resident of Minnesota on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Hill remains a Minnesota resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Hill: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Hill's data was "impacted."

w. Chris Tinen

70. Plaintiff Chris Tinen was a Missouri resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Tinen also was a resident of Missouri on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Tinen remains a Missouri resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Tinen: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Tinen's data was "impacted."

x. Kenneth Peterson

71. Plaintiff Kenneth Peterson was a Nevada resident during the period from mid-May through July 2017, when, according to Equifax, the data breach

occurred. Plaintiff Peterson also was a resident of Nevada on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Peterson remains a Nevada resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Peterson: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Peterson's data was "impacted." After learning of this breach, Plaintiff Peterson paid for credit freezes at the credit bureaus, in the total sum of $20.

y. Walter Kivlan

72. Plaintiff Walter Kivlan was a New Hampshire resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Kivlan also was a resident of New Hampshire on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Kivlan remains a New Hampshire resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Kivlan: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Kivlan's data was "impacted."

z. David Jungali

73. Plaintiff David Jungali was a New Jersey resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Jungali also was a resident of New Jersey on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Jungali remains a New Jersey resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Jungali: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Jungali's data was "impacted."

aa. Patricia Buhler

74. Plaintiff Patricia Buhler was a New York resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Buhler also was a resident of New York on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Buhler remains a New York resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Buhler: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Buhler's data was "impacted."

bb. Emily Bosak

75. Plaintiff Emily Bosak was a North Carolina resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Bosak also was a resident of North Carolina on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Bosak remains a North Carolina resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Bosak: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Bosak's data was "impacted."

cc. Sean Bosak

76. Plaintiff Sean Bosak was a North Carolina resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Bosak also was a resident of North Carolina on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Bosak remains a North Carolina resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Bosak: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Bosak's data was "impacted."

dd. Justin Peltier

77. Plaintiff Justin Peltier was a North Dakota resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Peltier also was a resident of North Dakota on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Peltier remains a North Dakota resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Peltier: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Peltier's data was "impacted."

ee. Peter Maizitis

78. Plaintiff Peter Maizitis was an Ohio resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Maizitis also was a resident of Ohio on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Maizitis remains an Ohio resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Maizitis: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Maizitis' data was "impacted."

ff. Jerry Nutt

79. Plaintiff Jerry Nutt was an Oklahoma resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Nutt also was a resident of Oklahoma on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Nutt remains an Oklahoma resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Nutt: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Nutt's data was "impacted."

gg. Marie Chinander

80. Plaintiff Marie Chinander was an Oregon resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Chinander also was a resident of Oregon on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Chinander remains an Oregon resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Chinander: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Chinander's data was "impacted." After learning of this breach, Plaintiff Chinander paid for credit freezes at the credit bureaus, in the total sum of $20.

hh. Raymond McCartney

81. Plaintiff Raymond McCartney was a Pennsylvania resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff McCartney also was a resident of Pennsylvania on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff McCartney remains a Pennsylvania resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff McCartney: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff McCartney's data was "impacted." After learning of this breach, Plaintiff McCartney paid for credit freezes at the credit bureaus, in the total sum of $10.

ii. Patricia Maggiacomo

82. Plaintiff Patricia Maggiacomo was a Rhode Island resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Maggiacomo also was a resident of Rhode Island on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Maggiacomo remains a Rhode Island resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Maggiacomo: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Maggiacomo's data was "impacted."

jj. Michael Moore

83. Plaintiff Michael Moore was a South Carolina resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Moore also was a resident of South Carolina on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Moore remains a South Carolina resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Moore: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Moore's data was "impacted."

kk. David Steufen

84. Plaintiff David Steufen was a South Dakota resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Steufen also was a resident of South Dakota on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Steufen remains a South Dakota resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Steufen: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Steufen's data was "impacted." After learning of this breach, Plaintiff Steufen paid for credit freezes in the total sum of $10.00.

ll. Jeannie Baggett

85. Plaintiff Jeannie Baggett was a Tennessee resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Baggett also was a resident of Tennessee on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Baggett remains a Tennessee resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Baggett: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Baggett's data was "impacted."

mm. Cheryl Lawson

86. Plaintiff Cheryl Lawson was a Texas resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Lawson also was a resident of Texas on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Lawson remains a Texas resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Lawson: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Lawson's data was "impacted." After learning of this breach, Plaintiff Lawson paid for credit freezes at the credit bureaus, in the total sum of $20.83.

nn. Ivy Madsen

87. Plaintiff Ivy Madsen was a Utah resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Madsen also was a resident of Utah on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Madsen remains a Utah resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Madsen: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Madsen's data was "impacted."

oo. Scott Kingsland

88. Plaintiff Scott Kingsland was a Vermont resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Kingsland also was a resident of Vermont on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Kingsland remains a Vermont resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Kingsland: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Kingsland's data was "impacted."

pp. Georgeann Roberts

89. Plaintiff Georgeann Roberts was a Virginia resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Roberts also was a resident of Virginia on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Roberts remains a Virginia resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Roberts: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Roberts' data was "impacted." After learning of this breach, Plaintiff Roberts paid for credit freezes at the credit bureaus, in the total sum of $10.

qq. Peter de Jesus

90. Plaintiff Peter de Jesus was a Washington resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff de Jesus also was a resident of Washington on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff de Jesus remains a Washington resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff de Jesus: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff de Jesus's data was "impacted." After learning of this breach, Plaintiff de

Jesus paid for credit freezes at the credit bureaus. Plaintiff also paid $50 for credit monitoring.

rr. Zandra Mendoza

91. Plaintiff Zandra Mendoza was a Wisconsin resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Mendoza also was a resident of Wisconsin on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Mendoza remains a Wisconsin resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Mendoza: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Mendoza's data was "impacted."

ss. Tanya Palmer

92. Plaintiff Tanya Palmer was a West Virginia resident during the period from mid-May through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Palmer also was a resident of West Virginia on and around July 29, 2017, the date on which Equifax has reported that it learned of the data breach. Plaintiff Palmer remains a West Virginia resident. Per the Defendant's advice, Plaintiff used its "Check Potential Impact" tool at https://www.equifaxsecurity2017.com/potential-impact/. Defendant's tool returned the following message to Plaintiff Palmer: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Furthermore, because Equifax has reported that some 143 million

U.S. individuals' data was accessed via this breach, it is virtually certain that Plaintiff Palmer's data was "impacted."

93. Plaintiffs were harmed in having their personal and financial information compromised as a result of the data breach.

94. Plaintiffs would not have taken steps to protect their personal and financial information had Equifax informed them that it lacked an adequate computer network and data security to secure their and others' personal and financial information.

95. Plaintiffs suffered actual injury from having their financial and personal information compromised and stolen as a result of the data breach, and were further injured by Equifax's failure to provide timely and accurate notice that their data had been breached.

96. Plaintiffs suffered actual injury and damages as a result of the data breach that it would not have suffered: (1) had Equifax disclosed that it lacked the computer network and data security to adequately protect their personal and financial information, or (2) had Equifax provided timely and accurate notice that their data had been breached.

2. The Defendant

97. Defendant Equifax is a Delaware corporation with its principal place of business in Atlanta, Georgia.

IV. CLASS ALLEGATIONS

98. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action as a national class action for themselves and all members of the following Class of similarly situated individuals and entities:

The Nationwide Class[39]

All persons in the United States whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

99. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, which is a parent or subsidiary, or which is controlled by the Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

100. Plaintiffs also seek to certify the following Subclasses of the Nationwide Class (the "State Subclasses"):

The Alaska Subclass

All members of the Class who are residents of Alaska.

The Alabama Subclass

All members of the Class who are residents of Alabama.

The Arizona Subclass

All members of the Class who are residents of Arizona.

The Arkansas Subclass

All members of the Class who are residents of Arkansas.

The California Subclass

All members of the Class who are residents of California.

The Colorado Subclass

All members of the Class who are residents of Colorado

[39] Throughout this Complaint, Plaintiffs use the terms "Nationwide Class" and "Class" interchangeably to refer to the nationwide class defined in this paragraph.

The Connecticut Subclass

All members of the Class who are residents of Connecticut.

The Florida Subclass

All members of the Class who are residents of Florida.

The Georgia Subclass

All members of the Class who are residents of Georgia.

The Hawaii Subclass

All members of the Class who are residents of Hawaii.

The Idaho Subclass

All members of the Class who are residents of Idaho.

The Illinois Subclass

All members of the Class who are residents of Illinois.

The Indiana Subclass

All members of the Class who are residents of Indiana.

The Iowa Subclass

All members of the Class who are residents of Iowa.

The Kentucky Subclass

All members of the Class who are residents of Kentucky.

The Louisiana Subclass

All members of the Class who are residents of Louisiana.

The Maine Subclass

All members of the Class who are residents of Maine.

The Maryland Subclass

All members of the Class who are residents of Maryland.

The Massachusetts Subclass

All members of the Class who are residents of Massachusetts.

The Michigan Subclass

All members of the Class who are residents of Michigan.

The Minnesota Subclass

All members of the Class who are residents of Minnesota.

The Missouri Subclass

All members of the Class who are residents of Missouri.

The Nevada Subclass

All members of the Class who are residents of Nevada.

The New Hampshire Subclass

All members of the Class who are residents of New Hampshire.

The New Jersey Subclass

All members of the Class who are residents of New Jersey.

The New York Subclass

All members of the Class who are residents of New York.

The North Carolina Subclass

All members of the Class who are residents of North Carolina.

The North Dakota Subclass

All members of the Class who are residents of North Dakota.

The Ohio Subclass

All members of the Class who are residents of Ohio.

The Oklahoma Subclass

All members of the Class who are residents of Oklahoma.

The Oregon Subclass

All members of the Class who are residents of Oregon.

The Pennsylvania Subclass

All members of the Class who are residents of Pennsylvania.

The Rhode Island Subclass

All members of the Class who are residents of Rhode Island.

The South Carolina Subclass

All members of the Class who are residents of South Carolina.

The South Dakota Subclass

All members of the Class who are residents of South Dakota.

The Tennessee Subclass

All members of the Class who are residents of Tennessee.

The Texas Subclass

All members of the Class who are residents of Texas.

The Utah Subclass

All members of the Class who are residents of Utah.

The Vermont Subclass

All members of the Class who are residents of Vermont.

The Virginia Subclass

All members of the Class who are residents of Virginia.

The Washington Subclass

All members of the Class who are residents of Washington.

The Wisconsin Subclass

All members of the Class who are residents of Wisconsin.

The West Virginia Subclass

All members of the Class who are residents of West Virginia.

101. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

102. All members of the proposed Class and Subclasses are readily ascertainable. Equifax has access to addresses and other contact information for all members of the Class, which can be used for providing notice to Class and Subclass members.

103. ***Numerosity***. The Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Class members has not been determined at this time, Equifax has admitted that some 143 million records were breached. Given this enormous number, the state Subclasses will also be sufficiently numerous to merit class certification

104. ***Commonality***. Questions of law and fact common to all Class and Subclass members exist and predominate over any questions affecting only individual Class members, including, *inter alia*:

a. whether Equifax engaged in the wrongful conduct alleged herein;

b. whether Equifax's conduct was deceptive, unfair, and/or unlawful;

c. whether Equifax owed a duty to Plaintiffs and members of the Class to adequately protect their personal and financial information;

d. whether Equifax owed a duty to provide timely and accurate notice of the data breach to Plaintiffs and members of the Class;

e. whether Equifax used reasonable and industry-standard measures to protect Class members' personal and financial information;

f. whether Equifax knew or should have known that its data system was vulnerable to attack;

g. whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of tens of millions of Class members' personal and financial data;

h. whether Equifax should have notified the public immediately after it learned of the data breach;

i. whether Equifax violated state statutory consumer protection, consumer fraud, data-breach-notification, and other applicable laws;

j. whether Equifax violated state common law as to negligence and otherwise Georgia common law;

k. whether Plaintiffs and Class members are entitled to recover actual damages, statutory damages, and/or punitive damages; and

l. whether Plaintiffs and Class members are entitled to restitution, disgorgement, and/or other equitable relief.

105. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class members were injured through the uniform misconduct described above and assert the same claims for relief.

106. ***Adequacy***. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs have no interests

antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

107. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiffs and the Class members. Plaintiffs and the Class members have been harmed by Equifax's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Equifax's wrongful actions and/or inaction.

108. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

109. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2), because Equifax has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

110. The expense and burden of litigation would substantially impair the ability of Plaintiffs and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Equifax will retain the benefits of its wrongdoing despite its serious violations of the law.

V. COUNTS

COUNT I
NEGLIGENCE
(BROUGHT BY ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE NATIONWIDE CLASS, OR, ALTERNATIVELY, ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE STATE SUBCLASSES)

111. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

112. Plaintiffs bring this count on their own behalf and on behalf of the Nationwide Class under the laws of the State of Georgia, or, alternatively, on their own behalf and on behalf of the State Subclasses under the negligence laws of all 50 states and the District of Columbia.

113. By accepting and storing Plaintiffs' and the Nationwide Class and State Subclass members' non-public personal and financial information, including highly sensitive information such as Social Security numbers, driver's license numbers, dates of birth, street addresses, and account information, Equifax assumed a duty, including a special or fiduciary duty, to all Plaintiffs and the Nationwide Class and State Subclass members requiring it to use reasonable and, at the very least, industry-standard care to secure such information against theft and misuse.

114. Equifax breached its duty of care by failing to adequately secure and protect Plaintiffs' and the Nationwide Class and State Subclass members' personal and financial information from theft, access, collection, and misuse by third parties.

115. Further, Equifax breached its duty of care by failing to act to protect Plaintiffs' and the Nationwide Class State Subclass members' personal and financial information, including, upon information and belief, by neglecting to promptly, completely, and effectively patch and repair its systems when initially

advised of one or more critical flaws or vulnerabilities in the Apache Struts Web application framework that it used, or other flaws or vulnerabilities in Apache Struts, or flaws or vulnerabilities in other software, such that the referenced data breach has occurred.

116. Equifax further breached its duty of care by failing to promptly, timely, clearly, accurately, and completely inform Plaintiffs and the Class that their personal and financial information had been stolen.

117. Plaintiffs and members of the Nationwide Class and State Subclasses have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Equifax's negligence and misconduct.

118. As a direct and proximate result of Equifax's failure to take reasonable care and use at least industry-standard measures to protect the personal information placed in its care, Plaintiffs and members of the Nationwide Class and State Subclasses had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and threat of identity theft.

119. As a direct and proximate result of Equifax's negligence and misconduct, Plaintiffs and members of the Nationwide Class and State Subclasses were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, or PII, due to the data breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of

productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(BROUGHT BY ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE NATIONWIDE CLASS, OR, ALTERNATIVELY, ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE STATE SUBCLASSES)

120. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

121. Plaintiffs bring this count on their own behalf and on behalf of the Nationwide Class under the laws of the state of Georgia, or, alternatively, on their own behalf and on behalf of the State Subclasses under the negligence laws of all 50 states and the District of Columbia.

122. Pursuant to Section 5 of the Federal Trade Commission Act ("FTC Act"), and pursuant to the various state laws referred to and referenced below for such states ("State Laws"), Equifax had a duty to keep and protect the personal information of all Plaintiffs and Class members.

123. Equifax violated the FTC Act and the State Laws by failing to keep and protect Plaintiffs' and Class members' extremely sensitive and valuable personal and financial information, failing to monitor, and/or failing to ensure that it complied with data security standards, industry standards, statutes, and/or other regulations to protect such personal and financial information. All such omissions were patently unreasonable given the high stakes if malicious actors were to access such information, which they now have done.

124. Equifax's failure to comply with the FTC Act, State Laws, and/or other industry standards and regulations, constitutes negligence *per se*.

125. Equifax violated the FTC Act and the State Laws by failing to safe-keep and protect Plaintiffs' and Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with applicable and current data security standards, statutes, and/or other regulations to protect such personal and financial information.

126. Further, Equifax violated the FTC Act and the State Laws by failing to act to protect Class members' personal and financial information, including, upon information and belief, by neglecting to promptly patch and repair its systems when advised of one or more critical flaws or vulnerabilities in the Apache Struts Web application framework that it used, or other flaws or vulnerabilities in Apache Struts, or flaws or vulnerabilities in other software, such that the referenced data breach has occurred.

127. Equifax's failure to comply with the FTC Act, the State Laws, and/or other industry standards and regulations constitutes negligence *per se*.

128. Plaintiffs and members of the Nationwide Class and State Subclasses have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Equifax's negligence *per se*.

129. As a direct and proximate result of Equifax's negligence *per se*, Plaintiffs and members of the Nationwide Class and State Subclasses had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and threat of identity theft.

130. As a direct and proximate result of Equifax's negligence *per se*, Plaintiffs and members of the Nationwide Class and State Subclasses were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, or PII, due to the data breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related

to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT III
VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT
GA. CODE ANN. § 10-1-370, *ET SEQ.*
(BROUGHT BY ALL PLAINTIFFS ON THEIR OWN BEHALF AND ON BEHALF OF THE NATIONWIDE CLASS)

131. Plaintiffs incorporate the above allegations by reference.

132. Plaintiffs bring this Count on their own behalf and on behalf of the Nationwide Class

133. Equifax, a Georgia resident; the Georgia-Resident Plaintiff; and members of the Georgia Subclass are "persons" within the meaning of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. § 10-1-371(5).

134. The Georgia UDTPA prohibits "deceptive trade practices," which include the "misrepresentation of standard or quality of goods or services," and "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Ga. Code Ann. § 10-1-372(a).

135. In the course of its business, Equifax willfully failed to disclose and actively concealed its grave data-security defects as discussed herein, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or

practices, fraud, misrepresentations, or concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable personal and financial information of the Plaintiffs and Nationwide Class members. Equifax did all of this directly with respect to the Plaintiffs and Nationwide Class members, and also by way of their transactions as to goods, merchandise, and services with prospective creditors and creditors who also accessed their extremely sensitive and valuable personal and financial in the course of those transactions.

136. For months, Equifax knew of vulnerabilities and defects in its data-security systems, and vulnerabilities in key databases storing the extremely sensitive and valuable personal and financial information of the Plaintiffs and Nationwide Class members, but concealed all of that information.

137. Equifax was also aware that it valued profits over real and effective data security. Equifax concealed this information as well.

138. By way of the foregoing, Equifax engaged in deceptive business practices in violation of the Georgia UDTPA. Equifax also engaged in deceptive acts and practices in at least the following ways:

a. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Nationwide Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Nationwide Class members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Nationwide Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nationwide Class members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nationwide Class members' personal and financial information, with the intent that others rely on the omission, suppression, and concealment;

d. Equifax engaged in deceptive acts and practices by failing to maintain the privacy and security of Nationwide Class members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; and the Georgia Code (O.C.G.A.) § 10-1-911, *et seq.*;

e. Equifax engaged in deceptive acts and practices by failing to disclose the data breach to Nationwide Class members in a timely and accurate manner, in violation of Ga. Code Ann. § 10-1-912;

f. Equifax engaged in deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Nationwide Class members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

139. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including the Plaintiffs and Nationwide Class members, regarding the security and safety of its databases and the extremely sensitive and valuable personal and financial information of the Plaintiffs and Nationwide Class members.

140. Equifax intentionally and knowingly misrepresented such material facts with an intent to mislead the Plaintiffs and Nationwide Class members.

141. Equifax knew or should have known that its conduct violated the Georgia UDTPA.

142. As alleged above, Equifax made material statements that were either false or misleading.

143. Equifax owed the Plaintiffs and Nationwide Class a duty to disclose the true facts regarding data-security defects and vulnerabilities because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over the safety of the extremely sensitive and valuable personal and financial information of the Plaintiffs and Nationwide Class members;

b. Intentionally concealed the foregoing from the Plaintiffs and Nationwide Class; and/or

c. Made incomplete representations regarding these matters while purposefully withholding material facts from Plaintiffs and the Nationwide Class that contradicted these representations.

144. Equifax's representations and omissions were material to the Plaintiffs and Nationwide Class given the extreme sensitivity and value of their personal and financial information.

145. Plaintiffs and the Nationwide Class suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

146. Equifax had an ongoing duty to all Equifax customers, including Plaintiffs and the Nationwide Class members, to refrain from unfair and deceptive practices under the Georgia UDTPA.

147. Equifax's violations present a continuing risk to the Plaintiffs and Nationwide Class members, as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

148. As a direct and proximate result of Equifax's violations of the Georgia UDTPA, Plaintiffs and Nationwide Class members have suffered injury-in-fact and/or actual damage. Plaintiffs seek an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Georgia UDTPA per Ga. Code Ann. § 10-1-373.

COUNT IV
STATE CONSUMER PROTECTION LAWS
(BROUGHT BY THE STATE-RESIDENT PLAINTIFFS AND THE STATE SUBCLASSES BELOW)

A. Common Allegations

149. Each of the following allegations in this subheading are alleged and incorporated into the allegations in each state subheading as to such state's consumer protection statutes.

150. Equifax participated in misleading, false, or deceptive acts that violated state law. By claiming to adequately secure consumers' personal and financial information, when in truth and fact its security practices were inadequate, Equifax engaged in deceptive business practices prohibited by the laws of the states set forth below.

151. In the course of its business, Equifax stored and warehoused the personal and financial information of hundreds of thousands, if not millions, of consumers in the states listed below, yet it did not take adequate steps to protect such data from theft, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or

concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its provision of credit bureau services to citizens and businesses in the following states.

152. Equifax has known of its inadequate data security at least since March 2017, but it concealed all of that information until recently.

153. Equifax was also aware that it suffered a data breach in March 2017, and again in May through July 2017, yet it valued profits over protecting consumers' personal and financial information, and concealed its data breaches for months, giving criminals ample time to steal 143 million accounts, which included highly valuable data elements, such as SSNs, DOBs, and DLNs.

154. By failing to disclose and by actively concealing its deficient data security and its data breaches, by marketing its computer systems and data storage as safe, reliable, and of high quality, and by presenting itself as a reputable credit bureau that valued data protection and stood behind consumers, Equifax engaged in deceptive, unfair, and unconscionable business practices in violation of the laws of the states set forth below.

155. In the course of Equifax's business, it willfully failed to disclose and actively concealed that it was not taking industry-standard and reasonable steps to protect the personal and financial information of at least 143 million consumers. Equifax compounded the deception by failing to disclose multiple data breaches, including the massive data breach that resulted in the theft of 143 million consumers' personal and financial information as well as a large number of credit card numbers.

156. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiffs and members of each of the state Subclasses, about the true security of its data systems, the ability of

Equifax to provide data security and identity-theft prevention services, and the integrity of the Equifax company.

157. Equifax intentionally and knowingly misrepresented material facts regarding its services and its ability to protect consumers' personal and financial information with an intent to mislead Plaintiffs and the state Subclasses.

158. Additionally, by way of these unfair, unlawful, and deceptive acts and practices, Equifax violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; and state data breach laws, including but not limited to those enumerated in the State Subclass claims below.

159. Equifax knew or should have known that its conduct violated the state statutes set forth below.

160. Equifax made material statements about the security and reliability of its computer and data systems and Equifax services that were either false or misleading.

161. Equifax owed Plaintiffs a duty to disclose the true nature and extent of its computer and data system security and that it had suffered data breaches, because Equifax:

a. Possessed exclusive knowledge that it valued profits over the bona fide protection of consumers' personal and financial information and that it had suffered multiple data breaches;

b. Intentionally concealed the foregoing from Plaintiffs; and/or

c. Made incomplete representations about the security of its computer and data systems, while purposefully withholding material facts from Plaintiffs that contradicted these representations.

162. Because Equifax fraudulently concealed its deficient computer and data security and its data breaches, resulting in the theft of personal and financial

information of 143 million consumers, Plaintiffs and the state Subclasses listed below have been harmed.

163. Equifax's deficient computer and data security and its concealment of its data breaches were material to Plaintiffs and the state Subclasses. Plaintiffs and members of the state Subclasses would have taken steps to protect their personal and financial information had they known that it was at risk, and in fact had been stolen from Equifax's computer and data systems.

164. Plaintiffs and the state Subclasses suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Class members have spent hours attempting to protect themselves from identity theft and have spent money to initiate credit freezes and taken other reasonable steps to limit their exposure to identity and credit theft.

165. Equifax had an ongoing duty to all persons about whom it maintained credit files to refrain from unfair and deceptive acts or practices under the state laws set forth below. All persons whose data was stolen in the data breach suffered ascertainable loss in the form of their loss of time, out-of-pocket expenses for credit freezes and identity-theft protection, and/or continuing and heightened risk of identity theft. Additionally, all Plaintiffs, Nationwide Class members, and State Subclass members have lost the monetary value, including the market value, of their personal and financial information, or PII, due to the data breach which has led to, or will lead to, its sale on the black market or its presence on dark web sites.

B. Alabama

VIOLATION OF ALABAMA CONSUMER PROTECTION ACT ALA. CODE 1975 § 18-19-1, ET SEQ. (BROUGHT BY THE ALABAMA-RESIDENT PLAINTIFF AND THE ALABAMA SUBCLASS)

166. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

167. Plaintiff Diane Brown is a resident of Alabama and was also a resident of Alabama when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Alabama Subclass.

168. The Alabama Unfair Trade Practices Act (AUTPA) prohibits the following conduct in trade or commerce:

> (2) Causing confusion or misunderstanding as to the source, sponsorship, approval, or certification of goods or services.
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have. . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (27) Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

ALA. CODE § 8-19-5.

169. Equifax's acts and omissions affect trade and commerce and affect sponsorship of goods and services in Alabama.

170. Equifax has committed acts of unfair competition in violation of ALA. CODE § 8-19-5. Equifax falsely represented to the Alabama-Resident Plaintiff and the Alabama Subclass[40] that personal and financial information provided to Equifax in sales transactions would be safe and secure from theft and unauthorized use when, in truth and fact, Equifax did not take reasonable and industry-standard measures to protect such personal and financial information from theft and misuse. Furthermore, Equifax failed to purge and delete personal information of former customers from its computer systems even though it no longer had any legitimate

[40] Throughout this Complaint, references to a Subclass also include the State-Resident Plaintiff(s).

business reason to maintain that data. Finally, Equifax induced customers into transactions by willfully omitting that its security systems were insufficient to safeguard their data.

171. Equifax has violated ALA. CODE § 8-19-5 (2) and (5) through its representations that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that it do not have…"

172. Equifax has also violated ALA. CODE § 8-19-5 (7) because it represented that its goods and services were of a particular standard, quality or grade, when in truth and fact, they were not.

173. Equifax has also violated ALA. CODE § 8-19-5 (9) because it induced transactions with consumers under the false auspices that it reasonably protected consumers' private data.

174. Equifax conducted the practices alleged herein in the course of its business, pursuant to standardized practices that it engaged in both before and after the Plaintiffs in this case were harmed, these acts have been repeated millions of times, and many consumers were affected.

175. Equifax's misrepresentations and omissions were material to the Alabama-Resident Plaintiff and the Alabama Subclass's transactions with Equifax and were made knowingly and with reason to know that the Alabama-Resident Plaintiff and the Alabama Subclass would rely on the misrepresentations and omissions.

176. The Alabama-Resident Plaintiff and the Alabama Subclass reasonably relied on Equifax's misrepresentations and omissions and suffered harm as a result. The Alabama-Resident Plaintiff and the Alabama Subclass were injured in fact by: fraudulent charges on their accounts; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition

of withdrawal and purchase limits on compromised accounts; (e) inability to withdraw funds held in linked checking accounts; (f) trips to banks and waiting in line to obtain funds held in limited accounts; (g) resetting automatic billing instructions; (h) late fees and declined payment fees imposed as a result of failed automatic payments; (i) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (j) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

177. The Alabama-Resident Plaintiff and the Alabama Subclass seek actual and statutory damages, to the full extent permitted under applicable law.

C. Alaska

VIOLATION OF ALASKA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT ALASKA STAT. § 45.50.531 (BROUGHT BY THE ALASKA-RESIDENT PLAINTIFF AND THE ALASKA SUBCLASS)

178. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

179. Plaintiff David Horne is a resident of Alaska and was also a resident of Alaska when the data breach occurred. Plaintiff Horne brings this Count on his own behalf and on behalf of members of the Alaska Subclass.

180. The Alaska Unfair Trade Practices and Consumer Protection Act ("UTPCPA") declares unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce unlawful, including "(4) representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not

have"; and "(12) using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression or omission in connection with the sale or advertisement of goods or services whether or not a person has in fact been misled, deceived or damaged." ALASKA STAT. § 45.50.471.

181. For the reasons discussed above, Equifax violated (and, on information and belief, continues to violate) the Alaska UTPCPA by engaging in the above-described and prohibited unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

182. Equifax violated the UTPCPA by accepting and storing Plaintiffs' and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Equifax also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards, and data security in place.

183. Equifax also violated the UTPCPA by failing to immediately notify Plaintiffs and the Class of the data breach. If Plaintiffs and the Class had been notified in an appropriate fashion, they could have taken precautions to better safeguard their personal and financial information.

184. Equifax's above-described wrongful acts and practices constitute "unfair" business acts and practices, in that they have the capacity or tendency to deceive. *State v. O'Neill Investigations, Inc.*, 609 P.2d 520, 534 (Alaska 1980). The harm caused by Equifax's above wrongful conduct outweighs any utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral, unscrupulous, unethical, oppressive, deceitful, and offensive, and/or (iii) has caused (and will continue to cause) substantial injury to consumers, such as

Plaintiffs and the Class. There were reasonably available alternatives to further Equifax's legitimate business interests, including using best practices to protect the personal and financial information, other than Equifax's wrongful conduct described herein.

185. "A person who suffers an ascertainable loss of money or property as a result of another person's act or practice declared unlawful by ALASKA STAT. 45.50.471 may bring a civil action to recover for each unlawful act or practice three times the actual damages or $500, whichever is greater. The court may provide other relief it considers necessary and proper." ALASKA STAT. § 45.50.531(a). Attorneys' fees may also be awarded to the prevailing party. ALASKA STAT. § 45.50.531(g).

186. On information and belief, Equifax's unlawful, fraudulent, and unfair business acts and practices, except as otherwise indicated herein, continue to this day and are ongoing. As a direct and/or proximate result of Equifax's unlawful, unfair, and fraudulent practices, Plaintiffs and the Class have suffered injury in fact and lost money in connection with the data breach, for which they are entitled to compensation – as well as restitution, disgorgement, and/or other equitable relief. Plaintiffs and the Class were injured in fact by: fraudulent charges on their accounts; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; (e) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (f) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

D. Arizona

VIOLATION OF ARIZONA CONSUMER FRAUD ACT
A.R.S. § 44-1521, *ET SEQ.*
(BROUGHT BY THE ARIZONA-RESIDENT PLAINTIFF AND THE ARIZONA SUBCLASS)

187. Plaintiffs incorporate the above allegations by reference.

188. Plaintiff Kelly Flood is a resident of Arizona and was also a resident of Arizona when the data breach occurred. Plaintiff Flood brings this Count on her own behalf and on behalf of members of the Arizona Subclass.

189. Equifax engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" in violation of Ariz. Rev. Stat. §44-1522(A), in at least the following ways:

a. Equifax misrepresented material facts to creditors selling merchandise to the Arizona Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Arizona Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft, and that it would comply with relevant federal and state law pertaining to such information;

b. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Arizona Subclass members' personal and financial information, with the intent that others rely on the omission, suppression, and concealment;

c. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Arizona Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act

(15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule.

190. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

191. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Arizona Subclass members' personal and financial information, and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Arizona Subclass.

192. As a direct and proximate result of Defendant's unfair and deceptive practices and acts, Arizona Subclass members suffered injury and/or damages.

193. Arizona Subclass members seek relief including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

E. Arkansas

VIOLATION OF ARKANSAS DECEPTIVE TRADE PRACTICES ACT ARK. CODE ANN. § 4-88-107(a)(10) (BROUGHT BY THE ARKANSAS-RESIDENT PLAINTIFF AND THE ARKANSAS SUBCLASS)

194. Plaintiffs incorporate the above allegations by reference.

195. Plaintiff Thurman Bryan Clark is a resident of Arkansas and was also a resident of Arkansas when the data breach occurred. Plaintiff Clark brings this Count on his own behalf and on behalf of members of the Arkansas Subclass.

196. The Arkansas Deceptive Trade Practices Act ("DTPA") prohibits "deceptive and unconscionable trade practices," which include but are not limited to a list of enumerated items, including "[e]ngaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade[.]" Ark. Code Ann. § 4-88-107(a)(10).

197. The Arkansas-Resident Plaintiff, members of the Arkansas Subclass, and the Defendant are "persons" within the meaning of the DTPA. Ark. Code Ann. § 4-88-102(5).

198. The conduct of Equifax as set forth herein constitutes deceptive and unconscionable trade practices because it failed to adequately investigate, disclose, and remedy the serious security flaws and vulnerabilities inherent in its data storage facilities and applications allowing access to the extremely sensitive and valuable personal and financial information of the Arkansas Subclass, and its misrepresentations and omissions regarding the safety and security of its data-access applications and data storage also constitute unconscionable or deceptive trade practices.

199. Defendant's conduct was unconscionable because it affronts the sense of justice, decency, or reasonableness, including as established by public policy and the state and federal laws enumerated herein. Defendant's unconscionable and deceptive trade practices occurred or were committed in the course, vocation, or occupation of its business, commerce, or trade. Defendant is directly liable for these violations of law.

200. Defendant engaged in a deceptive trade practice when it failed to disclose material information concerning the vulnerability to attack of its data-access applications and data storage facilities, intending that consumers and prospective and actual creditors would rely on that omission, in order to continue to profit from the personal and financial information of the Arkansas Subclass.

201. The information withheld was material in that it was information that was vitally important to consumers. Defendants' withholding of this information was likely to mislead consumers acting reasonably under the circumstances. Defendants' conduct proximately caused injuries to the Arkansas-resident Plaintiff and Arkansas Subclass.

202. Arkansas-resident Plaintiff and the Arkansas Subclass were injured as a result of Defendant's conduct as alleged herein. These injuries are the direct and natural consequence of Equifax's unconscionable conduct, misrepresentations, and omissions.

203. The Arkansas-Resident Plaintiff and other members of the Arkansas Subclass are entitled to recover actual damages, as well as reasonable attorneys' fees, for Defendant's unlawful conduct.

F. California

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §17200, *ET SEQ.* (BROUGHT BY THE CALIFORNIA-RESIDENT PLAINTIFFS AND THE CALIFORNIA SUBCLASS)

204. Plaintiffs incorporate the above allegations by reference.

205. Plaintiffs Debbie Person and Amanda Chap are residents of California and were also residents of California when the data breach occurred. Plaintiffs bring this Count on their own behalf and on behalf of members of the California Subclass.

206. Equifax operates in California and has violated Cal. Bus. and Prof. Code §17200, *et seq.*, by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code §17200 with respect to its activities pertaining to the California Subclass, in at least the following ways:

a. Equifax engaged in deceptive acts and practices by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard California Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft; and representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of California Subclass members' personal and financial information.

b. Equifax engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass members' personal and financial information with knowledge that the information would not be adequately protected; and by storing California Subclass members' personal and financial information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and California's data breach statute, Cal. Civ. Code § 1798.81.5. The harm these practices caused to Plaintiffs and the California Subclass members outweighed their utility, if any.

c. Equifax engaged in unfair acts and practices by failing to disclose the data breach to California Subclass members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass members. The harm these practices caused to Plaintiffs and the California Subclass members outweighed their utility, if any.

d. Equifax engaged in unfair acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect California Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass members. The harm these practices caused to Plaintiffs and the California Subclass members outweighed their utility, if any.

207. As a direct and proximate result of Defendant Equifax's acts of unfair and unlawful practices, the Plaintiffs were injured and lost money or property. Plaintiffs also lost their legally protected interest in the confidentiality and privacy of their personal and financial information, and additional losses described above.

208. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass members' personal and financial data, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

209. California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiffs and California Subclass members of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorney's fees and

costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

G. Colorado

VIOLATION OF COLORADO CONSUMER PROTECTION ACT COLO. REV. STAT. § 6-1-101, *ET. SEQ.* (BROUGHT BY THE COLORADO-RESIDENT PLAINTIFF AND THE COLORADO SUBCLASS)

210. Plaintiffs incorporate the above allegations by reference.

211. Plaintiff Timothy Hutz is a resident of Colorado and was also a resident of Colorado when the data breach occurred. Plaintiff Hutz brings this Count on his own behalf and on behalf of members of the Colorado Subclass.

212. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the course of Defendant's business, vocation, or occupation, in violation of Colo. Rev. Stat. § 6-1-105, in at least the following ways:

a. Equifax knowingly misrepresented and fraudulently advertised material facts by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Colorado Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft, in violation of Colo. Rev. Stat. § 6-1-105(1)(e), (g), (i), and (u);

b. Equifax knowingly misrepresented material facts by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Colorado Subclass members' personal and financial information, in violation of Colo. Rev. Stat. § 6-1-105(1)(e), (g), (i), and (u);

c. Equifax knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Colorado Subclass members' personal and financial information (intending to induce others to enter into a transaction), in violation of Colo. Rev. Stat. § 6-1-105(1)(e), (g), (i), and (u);

d. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to maintain the privacy and security of Colorado Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to disclose the data breach to Colorado Subclass members in a timely and accurate manner, contrary to the duties imposed by Colo. Rev. Stat. § 6-1-716(2).

f. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of Colo. Rev. Stat. § 6-1-105(3), by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Colorado Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

213. Defendant engaged in the above unfair or deceptive acts or practices in the course of their business.

214. As a direct and proximate result of Defendant's deceptive trade practices, Colorado Subclass members suffered injuries to legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal and financial information.

215. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

216. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Colorado Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Colorado Subclass.

217. Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-101, *et. seq*., including, not limited to, compensatory damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

H. Connecticut

VIOLATION OF CONNECTICUT UNFAIR TRADE PRACTICES ACT C.G.S. § 42-110A *ET SEQ.*, (BROUGHT BY THE CONNECTICUT-RESIDENT PLAINTIFF AND THE CONNECTICUT SUBCLASS)

218. Plaintiffs incorporate the above allegations by reference.

219. Plaintiff Lea Santello is a resident of Connecticut and was also a resident of Connecticut when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Connecticut Subclass.

220. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Conn. Gen. Stat. § 42-110b, in at least the following ways:

a. Equifax misrepresented and fraudulently advertised material facts to the Connecticut Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Connecticut Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to the Connecticut Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Connecticut Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Connecticut Subclass members' personal and financial information;

d. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Connecticut Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Connecticut data breach statute (Conn. Gen. Stat. § 42-471).

e. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Connecticut Subclass members in a timely and accurate manner, contrary to the duties imposed by Conn. Gen. Stat. § 36a-701b.

f. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Connecticut Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

221. As a direct and proximate result of Defendant's deceptive trade practices, Connecticut Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally

protected interest in the confidentiality and privacy of their personal and financial information.

222. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

223. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Connecticut Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Connecticut Subclass.

224. Connecticut Subclass members seek relief under Conn. Gen. Stat. § 42-110a, *et seq.*, including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

I. Florida

VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, FLA. STAT. § 501.201, ET SEQ., AND THE UNFAIR TRADE PRACTICES STATUTES (BROUGHT BY THE FLORIDA-RESIDENT PLAINTIFF AND THE FLORIDA SUBCLASS)

225. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

226. Plaintiff Lisa Melegari is a resident of Florida and was also a resident of Florida when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Florida Subclass.

227. At all relevant times, Equifax provided goods and/or services and thereby was engaged in trade or commerce.

228. At all relevant times, Plaintiff and the Florida Subclass members were consumers.

229. Equifax was aware that consumers provided and it collected confidential and non-public information and personally identifiable material in connection with Equifax's business in Florida.

230. Plaintiff and the Florida Subclass expected, and Equifax assured, that personal and financial information and non-public information maintained by Equifax would be protected and that it would not be disclosed to third parties.

231. Equifax engaged in unfair or deceptive acts and practices by knowingly permitting the personal and financial information to be exposed through a network that was unsecure or had inadequate safeguards, resulting in the dissemination of private personal and financial information of customers in direct violation of the Unfair Trade Practices Statutes.

232. Equifax engaged in unfair or deceptive acts and practices by failing to timely notify Plaintiff and the Florida Subclass of the security breach and compromise.

233. Equifax's practice and course of conduct, as alleged herein, is likely to mislead—and has misled—the consumer acting reasonably in the circumstances, to the consumer's detriment.

234. Further, Defendant has engaged in an unfair practice that offends established public policy, and is one that is immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to customers.

235. As a direct and proximate result of Equifax's conduct, Plaintiff and the Florida Subclass members suffered actual damages and request a corresponding award of damages against Defendant, as authorized by such statutes.

236. In the alternative, Plaintiff and the Florida Subclass members have suffered irreparable harm for which there is no adequate remedy at law as a result

of Defendant's conduct, and Plaintiff and the Florida Subclass members are entitled to appropriate temporary and permanent injunctive relief, as authorized and provided by such statutes. Plaintiff and the Florida Subclass members are further entitled to preliminary or other relief as provided by such statutes, including statutory damages, punitive damages, costs, and reasonable attorneys' fees.

J. Georgia

VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT
GA. CODE ANN. § 10-1-370, *ET SEQ.*
(BROUGHT BY THE GEORGIA-RESIDENT PLAINTIFF AND THE GEORGIA SUBCLASS)

237. Plaintiffs incorporate the above allegations by reference.

238. Plaintiff Dawn Evans is a resident of Georgia and was also a resident of Georgia when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Georgia Subclass.

239. Equifax, a Georgia resident; the Georgia-Resident Plaintiff; and members of the Georgia Subclass are "persons" within the meaning of Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. § 10-1-371(5).

240. The Georgia UDTPA prohibits "deceptive trade practices," which include the "misrepresentation of standard or quality of goods or services," and "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Ga. Code Ann. § 10-1-372(a).

241. In the course of its business, Equifax willfully failed to disclose and actively concealed its grave data-security defects as discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material

facts with intent that others rely upon such concealment, suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable personal and financial information of the Georgia-Resident Plaintiff and Georgia Subclass members. Equifax did all of this directly with respect to the Georgia-Resident Plaintiff and Georgia Subclass members, and also by way of their transactions as to goods, merchandise, and services with prospective creditors and creditors who also accessed their extremely sensitive and valuable personal and financial in the course of those transactions.

242. For months, Equifax knew of vulnerabilities and defects in its data-security systems, and vulnerabilities in key databases storing the extremely sensitive and valuable personal and financial information of the Georgia-Resident Plaintiff and Georgia Subclass members, but it concealed all of that information.

243. Equifax was also aware that it valued profits over real and effective data security. Equifax concealed this information as well.

244. By way of the foregoing, Equifax engaged in deceptive business practices in violation of the Georgia UDTPA. Equifax also engaged in deceptive acts and practices in at least the following ways:

a. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Georgia Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Georgia Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Georgia Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Georgia Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Georgia Subclass members' personal and financial information, with the intent that others rely on the omission, suppression, and concealment;

d. Equifax engaged in deceptive acts and practices by failing to maintain the privacy and security of Georgia Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; and Ga. Code Ann. § 10-1-911, *et seq.*;

e. Equifax engaged in deceptive acts and practices by failing to disclose the data breach to Georgia Subclass members in a timely and accurate manner, in violation of Ga. Code Ann. § 10-1-912;

f. Equifax engaged in deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Georgia Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

245. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including the Georgia-Resident Plaintiff and other members of the Georgia Subclass, regarding the security and safety of its databases and the extremely sensitive and valuable personal and financial information of the Georgia-Resident Plaintiff and Georgia Subclass members.

246. Equifax intentionally and knowingly misrepresented such material facts with an intent to mislead the Georgia-Resident plaintiff and the Georgia Subclass.

247. Equifax knew or should have known that its conduct violated the Georgia UDTPA.

248. As alleged above, Equifax made material statements that were either false or misleading.

249. Equifax owed the Georgia-Resident Plaintiff and the Georgia Subclass a duty to disclose the true facts regarding data-security defects and vulnerabilities because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over the safety of the extremely sensitive and valuable personal and financial information of the Georgia-Resident Plaintiff and Georgia Subclass members;

b. Intentionally concealed the foregoing from the Georgia-Resident Plaintiff and the Georgia Subclass; and/or

c. Made incomplete representations regarding these matters while purposefully withholding material facts from Plaintiffs and the Class that contradicted these representations.

250. Equifax's representations and omissions were material to Plaintiff and the Georgia Subclass given the extreme sensitivity and value of their personal and financial information.

251. Plaintiff and the Georgia Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

252. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Georgia UDTPA.

253. Equifax's violations present a continuing risk to the Georgia-Resident Plaintiff and the Georgia Subclass, as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

254. As a direct and proximate result of Equifax's violations of the Georgia UDTPA, Plaintiffs and the Georgia Subclass have suffered injury-in-fact and/or actual damage. Plaintiffs seek an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Georgia UDTPA per Ga. Code Ann. § 10-1-373.

K. Hawaii

VIOLATION OF HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION STATUTE HAW. REV. STAT. § 480-1, *ET SEQ.* (BROUGHT BY THE HAWAII-RESIDENT PLAINTIFF AND THE HAWAII SUBCLASS)

255. Plaintiffs incorporate the above allegations by reference.

256. Plaintiff Jennifer Griffin is a resident of Hawaii and was also a resident of Hawaii when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Hawaii Subclass.

257. Hawaii Subclass members are "consumers" as meant by Haw. Rev. Stat. § 480-1.

258. Hawaii Subclass members purchased "goods and services" from Defendant as meant by Haw. Rev. Stat. § 480-1.

259. Hawaii Subclass members' personal and financial information was accessed and stored by Defendant for personal, family, and/or household purposes, as meant by Haw. Rev. Stat. § 480-1.

260. Equifax engaged in unfair methods of competition, unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Hawaii Subclass in violation of Haw. Rev. Stat. § 480-2(a), in at least the following ways:

a. Equifax misrepresented and fraudulently advertised material facts to the Hawaii Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Hawaii Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to the Hawaii Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Hawaii Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Hawaii Subclass members' personal and financial information;

d. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Hawaii Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule,

e. Equifax engaged in unfair acts and practices by failing to disclose the data breach to Hawaii Subclass members in a timely and accurate manner, in violation of Haw. Rev. Stat. § 487N-2(a);

f. Equifax engaged in unfair acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Hawaii Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

261. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

262. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Hawaii Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Hawaii Subclass.

263. As a direct and proximate result of Defendant's unlawful practices, Hawaii Subclass members suffered injury and/or damages.

264. Hawaii Subclass members seek relief under Haw. Rev. Stat. § 480-13, including, but not limited to, damages, injunctive relief, statutory damages as permitted by applicable law, attorneys' fees and costs, and treble damages.

L. Idaho

VIOLATION OF PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT IDAHO CODE § 48-601, ET SEQ. (BROUGHT BY THE IDAHO-RESIDENT PLAINTIFF AND THE IDAHO SUBCLASS)

265. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

266. Plaintiff William Knudsen is a resident of Idaho and was also a resident of Idaho when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Idaho Subclass.

267. The Idaho Consumer Protection Act (ICPA) prohibits the following conduct in trade or commerce:

(2) Causing likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services;

(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that it do not have or that a person has a sponsorship, approval, status, affiliation, connection, qualifications or license that he does not have;

(7) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;

(9) Advertising goods or services with intent not to sell them as advertised;

(17) Engaging in any act or practice which is otherwise misleading, false, or deceptive to the consumer;

(18) Engaging in any unconscionable method, act or practice in the conduct of trade or commerce as provided in section 48-603C, Idaho Code.

IDAHO CODE § 48-603.

268. Equifax's acts and omissions affect trade and commerce and affect sponsorship of goods and services in Idaho.

269. Equifax has committed acts of unfair competition by: (1) representing to Plaintiff and the Idaho Subclass that personal and financial information provided to Equifax in sales transactions would be safe and secure from theft and unauthorized use when in truth and fact Equifax did not take reasonable and industry-standard measures to protect such personal and financial information from theft and misuse; and (2) by failing to purge and delete the personal information of former customers from its computer systems. Equifax has violated IDAHO CODE § 48-603(2) and (5) through its representations that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that it does not have…"

270. Equifax has also violated IDAHO CODE § 48-603(7) because it represented that its goods and services were of a particular standard, quality or grade, when in truth and fact, they were not.

271. Equifax has also violated IDAHO CODE § 48-603(9) and (17), because it induced transactions with consumers under the false auspices that it reasonably protected consumers' private data.

272. Equifax has also violated IDAHO CODE § 48-603(18) by unconscionably failing to protect its consumers' data.

273. Equifax conducted the practices alleged herein in the course of its business, pursuant to standardized practices that it engaged in both before and after the Plaintiff and the Idaho Subclass in this case were harmed, these acts have been repeated millions of times, and many consumers were affected.

274. Equifax's misrepresentations and omissions were material to Plaintiff and the Idaho Subclass members' transactions with Equifax and were made knowingly and with reason to know that Plaintiff and the Idaho Subclass would rely on the misrepresentations and omissions.

275. Plaintiff and the Idaho Subclass reasonably relied on Equifax's misrepresentations and omissions and suffered harm as a result. Plaintiff and the Idaho Subclass were injured in fact by: fraudulent charges on their accounts; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; (e) inability to withdraw funds held in linked checking accounts; (f) trips to banks and waiting in line to obtain funds held in limited accounts; (g) resetting automatic billing instructions; (h) late fees and declined payment fees imposed as a result of failed automatic payments; (i) the general nuisance and annoyance of dealing with all these issues resulting from the

data breach; and (j) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

276. Idaho-Resident Plaintiff and the Idaho Subclass seek all remedies available under applicable law including damages, statutory damages, restitution, attorneys' fees and costs of suit.

M. Illinois

VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 ILCS 505/1, ET SEQ. AND 720 ILCS 295/1A (BROUGHT BY THE ILLINOIS-RESIDENT PLAINTIFF AND THE ILLINOIS SUBCLASS)

277. Plaintiffs incorporate the above allegations by reference.

278. Plaintiff Scott Sroka is a resident of Illinois and was also a resident of Illinois when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Illinois Subclass.

279. Defendant is a "person" as that term is defined in 815 ILCS 505/1(c).

280. Plaintiff and the Illinois Subclass are "consumers" as that term is defined in 815 ILCS 505/1(e).

281. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Illinois CFA") prohibits "unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact … in the conduct of trade or commerce … whether any person has in fact been misled, deceived or damaged thereby." 815 ILCS 505/2.

282. Equifax participated in misleading, false, or deceptive practices that violated the Illinois CFA. By failing to disclose and actively concealing that its storage of the Illinois Subclass's personal and financial information was unsafe and vulnerable to attack, and by instead holding itself out as a safe and secure repository of this extremely sensitive and valuable data, Equifax engaged in deceptive business practices prohibited by the Illinois CFA.

283. In the course of its business, Equifax willfully failed to disclose and actively concealed the defective data storage discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its access to, and storage of, consumers' personal and financial information.

284. Equifax also knew of prior breaches and vulnerabilities in Apache Struts, but it concealed critical information from the Illinois Subclass and from the prospective creditors and creditors with whom they dealt in consumer transactions.

285. Equifax was also aware that it valued profits over the safety of the personal and financial information of the Illinois Subclass. Equifax concealed this information as well.

286. By all of the failures to disclose in the course of its business, and by actively concealing critical information as alleged herein, Equifax engaged in unfair and deceptive business practices in violation of the Illinois CFA.

287. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the other Illinois Subclass members, who were unaware of the true state of affairs with respect to the vulnerability of their critical personal and financial information.

288. Equifax intentionally and knowingly misrepresented material facts with an intent to mislead Plaintiff and the Illinois Subclass.

289. Equifax knew or should have known that its conduct violated the Illinois CFA.

290. As alleged above, Equifax made material statements about the safety of Plaintiff's and the Illinois Subclass's data, and Equifax security, that were either false or misleading.

291. Equifax owed Plaintiff and the Illinois Subclass a duty to disclose the true state of affairs to consumers because Equifax:

a. Possessed exclusive knowledge that it valued profits over truly effective data security;

b. Intentionally concealed the foregoing from Plaintiffs and the Illinois Subclass; and/or

c. Made incomplete representations about the safety of their data, while purposefully withholding material facts from Plaintiff and the Illinois Subclass that contradicted these representations.

292. Equifax's fraudulent behavior, in terms of the material concealed from the Illinois Class, and the misrepresentations and omissions made by Equifax, were material to Plaintiff and the Illinois Subclass.

293. Plaintiff and the Illinois Subclass suffered ascertainable loss and damages caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

294. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Illinois CFA. All Illinois Subclass members suffered ascertainable loss and damages as alleged herein as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

295. Equifax's violations present a continuing risk to the Illinois Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

296. As a direct and proximate result of Equifax's violations of the Illinois CFA, Plaintiff and the Illinois Subclass have suffered injury-in-fact and/or actual damage.

297. Pursuant to 815 ILCS 505/10a(a), Plaintiff and the Illinois Subclass seek monetary relief against Equifax in the amount of actual damages, as well as punitive damages because Equifax acted with fraud and/or malice and/or was grossly negligent.

298. Plaintiff and the Illinois Subclass also seek an order enjoining Equifax's unfair and/or deceptive acts or practices, punitive damages, and attorneys' fees, and any other just and proper relief available under the 815 ILCS 505/1 *et seq*.

N. Iowa

VIOLATIONS OF PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT IOWA CODE § 714H.1, ET SEQ. (BROUGHT BY THE IOWA-RESIDENT PLAINTIFF AND THE IOWA SUBCLASS)

299. Plaintiffs incorporate the above allegations by reference.

300. Plaintiff Patricia Tuel is a resident of Iowa and was also a resident of Iowa when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Iowa Subclass.

301. Defendant is a "person" under Iowa Code § 714H.2(7).

302. The Iowa-Resident Plaintiff and the Iowa Subclass are "consumers" as that term is defined by Iowa Code § 714H.2(3).

303. The Iowa Private Right of Action for Consumer Frauds Act ("Iowa CFA") prohibits any "practice or act the person knows or reasonably should know is an unfair practice, deception, fraud, false pretense, or false promise, or the misrepresentation, concealment, suppression, or omission of a material fact, with the intent that others rely upon the unfair practice, deception, fraud false pretense, false promise, misrepresentation, concealment, suppression, or omission in connection with the advertisement, sale or lease of consumer merchandise." Iowa Code § 714H.3.

304. Equifax participated in misleading, false, or deceptive practices that violated the Iowa CFA. By failing to disclose and actively concealing that access to and storage of the personal and financial information of the Iowa Subclass was not safe but was instead vulnerable to attack, by marketing its data storage and access as safe and of high quality, and by presenting itself as a reputable company that valued the safety of personal and financial information, Equifax engaged in deceptive business practices prohibited by the Iowa CFA.

305. In the course of its business, Equifax willfully failed to disclose and actively concealed the true nature of the safety of the Iowa Subclass's data as alleged herein, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with the personal and financial information of consumers as alleged herein.

306. As alleged herein, Equifax has known that its data storage and access facilities were unsafe because it experienced previous attacks, and because it was told of vulnerabilities in its applications, but it concealed all of that information.

307. Equifax was also aware that it valued profits over the safety of the Iowa Subclass's personal and financial information. Equifax concealed this information as well.

308. By failing to disclose that critical information as alleged herein, Equifax engaged in unfair and deceptive business practices in violation of the Illinois CFA.

309. In the course of Equifax's business, it willfully failed to disclose and actively concealed the dangerous risk posed by the vulnerabilities and deficiencies discussed above. Equifax compounded the deception by repeatedly asserting that Equifax applications and data storage were safe and reliable.

310. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the other Iowa Subclass members.

311. Equifax intentionally and knowingly misrepresented material facts regarding data security with an intent to mislead Plaintiff and the Iowa Subclass.

312. Equifax knew or should have known that its conduct violated the Iowa CFA.

313. As alleged above, Equifax made material statements about the safety of consumers' personal and financial information that were either false or misleading.

314. Equifax owed Plaintiff and the Iowa Subclass a duty to disclose critical information about access to and storage of the Iowa Subclass's personal and financial information because Equifax:

a. Possessed exclusive knowledge that it valued profits over true data safety and security;

b. Intentionally concealed information regarding data safety and security, and the safety and security of access to consumer data, from Plaintiff and the Iowa Subclass; and/or

c. Made incomplete representations about the safety and security of consumer data, while purposefully withholding material facts from Plaintiff and the Iowa Subclass that contradicted these representations.

315. Equifax's fraudulent misrepresentations and omissions were material to Plaintiff and the Iowa Subclass.

316. Plaintiff and the Iowa Subclass suffered ascertainable loss and damages caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

317. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Iowa CFA.

318. Equifax's violations present a continuing risk to the Iowa Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

319. As a direct and proximate result of Equifax's violations of the Iowa CFA, Plaintiff and the Iowa Subclass have suffered injury-in-fact and/or actual damage.

320. Pursuant to Iowa Code § 714H.5, Plaintiff and the Iowa Subclass seek an order enjoining Equifax's unfair and/or deceptive acts or practices; actual damages; in addition to an award of actual damages, statutory damages up to three times the amount of actual damages awarded as a result of Equifax's willful and wanton disregard for the rights and safety of others; attorneys' fees; and such other equitable relief as the Court deems necessary to protect the public from further violations of the Iowa CFA.

O. Kentucky

VIOLATION OF THE KENTUCKY CONSUMER PROTECTION ACT
KY. REV. STAT. § 367.110, *ET SEQ.*
(BROUGHT BY THE KENTUCKY-RESIDENT PLAINTIFF AND THE KENTUCKY SUBCLASS)

321. Plaintiffs incorporate the above allegations by reference.

322. Plaintiff Christopher Hutchison is a resident of Kentucky and was also a resident of Kentucky when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Kentucky Subclass.

323. Equifax, the Kentucky-Resident Plaintiff, and members of the Kentucky Subclass are "persons" within the meaning of the KY. REV. STAT. § 367.110(1).

324. Equifax engaged in "trade" or "commerce" within the meaning of KY. REV. STAT. § 367.110(2).

325. The Kentucky Consumer Protection Act ("Kentucky CPA") makes unlawful "[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce …." KY. REV. STAT. § 367.170(1). Equifax participated in misleading, false, or deceptive acts that violated the Kentucky CPA. By claiming to adequately secure consumers' personal and financial information, when in truth and fact its security practices were inadequate, Equifax engaged in deceptive business practices prohibited by the Kentucky CPA.

326. In the course of its business, Equifax stored and warehoused the personal and financial information of millions of Kentucky consumers, yet it did not take adequate steps to protect such data from theft, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in

connection with its provision of credit bureau services to Kentucky citizens and businesses.

327. Equifax has known of its inadequate data security at least since March 2017, but concealed all of that information until recently.

328. Equifax was also aware that it suffered a data breach in March 2017, and again in May through July 2017, yet it valued profits over protecting consumers' personal and financial information, and concealed its data breaches for months, giving criminals ample time to steal 143 million accounts, which included highly valuable data elements, such as SSNs, DOBs, and DLNs.

329. By failing to disclose and by actively concealing its deficient data security and its data breaches, by marketing its computer systems and data storage as safe, reliable, and of high quality, and by presenting itself as a reputable credit bureau that valued data protection and stood behind consumers, Equifax engaged in deceptive business practices in violation of the Kentucky CPA.

330. In the course of Equifax's business, it willfully failed to disclose and actively concealed that it was not taking industry-standard and reasonable steps to protect the personal and financial information of at least 143 million consumers. Equifax compounded the deception by failing to disclose multiple data breaches, including the massive data breach that resulted in the theft of 143 million consumers' personal and financial information.

331. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the Kentucky Subclass, about the true security of its data systems, the ability of Equifax to provide data security and identity-theft prevention services, and the integrity of the Equifax company.

332. Equifax intentionally and knowingly misrepresented material facts regarding its services and its ability to protect consumers' personal and financial information with an intent to mislead Plaintiff and the Kentucky Subclass.

333. Equifax knew or should have known that its conduct violated the Kentucky CPA.

334. Equifax made material statements about the security and reliability of its computer and data systems and Equifax services that were either false or misleading.

335. Equifax owed Plaintiff and the Kentucky Subclass a duty to disclose the true nature and extent of its computer and data system security and that it had suffered data breaches, because Equifax:

a. Possessed exclusive knowledge that it valued profits over the bona fide protection of consumers' personal and financial information and that it had suffered multiple data breaches;

b. Intentionally concealed the foregoing from Plaintiff and the Kentucky Subclass; and/or

c. Made incomplete representations about the security of its computer and data systems, while purposefully withholding material facts from Plaintiff and the Kentucky Subclass that contradicted these representations.

336. Because Equifax fraudulently concealed its deficient computer and data security and its data breaches, resulting in the theft of personal and financial information of 143 million consumers, Plaintiff and the Kentucky subclass have been harmed.

337. Equifax's deficient computer and data security and its concealment of its data breaches were material to Plaintiffs and the Kentucky Subclass. Plaintiffs and the Kentucky Subclass would have taken steps to protect their personal and

financial information had they known that it was at risk, and in fact had been stolen from Equifax's computer and data systems.

338. Plaintiffs and the Kentucky Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Plaintiff and the Kentucky Subclass members have spent hours attempting to protect themselves from identity theft and have spent money to initiate credit freezes and take other reasonable steps to limit their exposure to identity and credit theft.

339. Equifax had an ongoing duty to all persons about whom it maintained credit files to refrain from unfair and deceptive acts or practices under the Kentucky CPA. All persons whose data was stolen in the data breach suffered ascertainable loss in the form of their loss of time, out-of-pocket expenses for credit freezes and identity-theft protection, and continuing and heightened risk of identity theft.

340. Equifax's violations present a continuing risk to Plaintiff and the Kentucky Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

341. As a direct and proximate result of Equifax's violations of the Kentucky CPA, Plaintiff and the Kentucky Subclass have suffered injury-in-fact and/or actual damage.

342. Pursuant to KY. REV. STAT. ANN. § 367.220, Plaintiff and the Kentucky Subclass seek to recover actual damages in an amount to be determined at trial; an order enjoining Equifax's unfair, unlawful, and/or deceptive practices; declaratory relief; attorneys' fees; and any other just and proper relief available under KY. REV. STAT. ANN. § 367.220.

P. Louisiana

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW LA. REV. STAT. ANN. §51:1401, *ET SEQ*. (BROUGHT BY THE LOUISIANA-RESIDENT PLAINTIFF AND THE LOUISIANA SUBCLASS)

343. Plaintiffs incorporate the above allegations by reference.

344. Plaintiff Randi Freeman is a resident of Louisiana and was also a resident of Louisiana when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Louisiana Subclass.

345. Equifax, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. §51:1402(8).

346. Plaintiff and the Louisiana Subclass are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

347. Equifax engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

348. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Equifax participated in misleading, false, or deceptive acts that violated the Louisiana CPL.

349. In the course of its business, Equifax willfully failed to disclose and actively concealed the facts discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its use and storage of consumers personal and financial information.

350. Equifax knew it had not taken adequate steps to protect consumer's personal and financial information from theft, as represented. Equifax knew this for at least several months, but concealed all of that information.

351. Equifax was also aware that it valued profits over the security of consumers' personal and financial information, and that its data systems were not secure and that it had suffered multiple data breaches. Equifax concealed this information as well.

352. By failing to disclose that its computer and data systems were not secure, and by presenting itself as a reputable company that valued data security, Equifax engaged in deceptive business practices in violation of the Louisiana CPL.

353. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the other Louisiana Subclass members, about the true security of its computer and data systems and the devaluing data security at Equifax.

354. Equifax intentionally and knowingly misrepresented material facts regarding the security of consumers' personal and financial information with an intent to mislead Plaintiff and the Louisiana Subclass.

355. Equifax knew or should have known that its conduct violated the Louisiana CPL.

356. As alleged above, Equifax made material statements about the safety and security of personal and financial information that were either false or misleading.

357. Equifax owed the Louisiana Subclass a duty to disclose the true lack of security of its computer and data systems because Equifax:

a. Possessed exclusive knowledge that it valued profits over data security;

b. Intentionally concealed the foregoing from Plaintiff and the Louisiana Subclass; and/or

c. Made incomplete representations about the security of its computer and data systems generally, and that it had suffered data breaches in particular, while purposefully withholding material facts from Plaintiff and the Louisiana Subclass that contradicted these representations.

358. Equifax's fraudulent representations were material to Plaintiff and the Louisiana Subclass.

359. Plaintiff and the Louisiana Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein, including time and expenses associated with securing their identities from theft, including costs to implement and maintain credit freezes and identity theft monitoring and protection.

360. Equifax had an ongoing duty to all Louisiana Subclass members to refrain from unfair and deceptive practices under the Louisiana CPL. All members suffered ascertainable loss in the form of out-of-pocket costs and loss of time as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

361. Equifax's violations present a continuing risk to the Louisiana Subclass. Equifax's unlawful acts and practices complained of herein affect the public interest.

362. As a direct and proximate result of Equifax's violations of the Louisiana CPL, Plaintiff and the Louisiana Subclass have suffered injury-in-fact and/or actual damage.

363. Pursuant to La. Rev. Stat. Ann. § 51:1409, Plaintiff and the Louisiana Subclass seek to recover actual damages in an amount to be determined at trial; treble damages for Equifax's knowing violations of the Louisiana CPL; an order enjoining Equifax's unfair, unlawful, and/or deceptive practices; declaratory relief;

attorneys' fees; and any other just and proper relief available under La. Rev. Stat. Ann. § 51:1409.

Q. Maine

MAINE UNFAIR TRADE PRACTICES ACT
ME. REV. STAT. TIT. 5, § 205
(BROUGHT BY THE MAINE-RESIDENT PLAINTIFF AND THE MAINE SUBCLASS)

364. Plaintiffs incorporate the above allegations by reference.

365. Plaintiff Cassey-Jo Wood is a resident of Maine and was also a resident of Maine when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Maine Subclass.

366. Maine Subclass members' personal and financial information was accessed and stored by the Defendant for personal, family, and/or household purposes.

367. On September 22, Plaintiff Wood sent a demand for relief to Equifax on behalf of the Maine Subclass.

368. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Me. Rev. Stat. tit. 5, § 207, in at least the following ways:

a. Equifax misrepresented and fraudulently advertised material facts to the Maine Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Maine Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to the Maine Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maine Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Maine Subclass members' personal and financial information;

d. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Maine Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule.

e. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Maine Subclass members in a timely and accurate manner, contrary to the duties imposed by Me. Rev. Stat. tit. 10, § 1348(1);

f. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Maine Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

369. As a direct and proximate result of Defendant's deceptive trade practices, Maine Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

370. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

371. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Maine Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maine Subclass.

372. Maine Subclass members seek relief under Me. Rev. Stat. tit. 5, § 213, including, not limited to, damages, restitution, injunctive relief, and/or attorneys' fees and costs.

MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT ME. REV. STAT. TIT. 10, § 1212, *ET. SEQ.* (BROUGHT BY THE MAINE-RESIDENT PLAINTIFF AND THE MAINE SUBCLASS)

373. Plaintiffs incorporate the above allegations by reference.

374. Plaintiff Wood is a resident of Maine and was also a resident of Maine when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Maine Subclass.

375. While in the course of their businesses, Equifax engaged in deceptive trade practices by making false representations, including their representations that it had adequate computer systems and data security practices to protect personal and financial information, when its computer systems and data security practices were inadequate, in violation of Me. Rev. Stat. tit. 10, §1212(E),(G).

376. Defendant knew or should have known that its computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

377. Maine Subclass members are likely to be damaged by the Defendant's deceptive trade practices.

378. Maine Subclass members seek relief under Me. Rev. Stat. tit. 10, §1213, including, but not limited to, injunctive relief and attorney's fees.

R. Maryland

MARYLAND CONSUMER PROTECTION ACT
MD CODE COMMERCIAL LAW, § 13-301, *ET. SEQ.*
(BROUGHT BY THE MARYLAND-RESIDENT PLAINTIFF AND THE MARYLAND SUBCLASS)

379. Plaintiffs incorporate the above allegations by reference.

380. Plaintiff Donna Mosley is a resident of Maryland and was also a resident of Maryland when the data breach occurred. She brings this Count on her own behalf and on behalf of members of the Maryland Subclass.

381. Maryland Subclass members are "consumers" as meant by Md. Code Ann., Com. Law § 13-101.

382. The unlawful trade practices, misrepresentations, and omissions described herein did not constitute "professional services" on the part of Defendant.

383. Equifax engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Md. Code Ann., Com. Law § 13-301, in at least the following ways:

a. Equifax misrepresented material facts to the Maryland Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Maryland Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

b. Equifax misrepresented material facts to the Maryland Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maryland members' personal and financial information in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Maryland Subclass members' personal and financial information in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

d. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Maryland Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45); the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; Maryland's Privacy of Consumer Financial and Health Information regulations (Md. Code Regs. 31.16.08.01, et seq.); Maryland's data breach statute (Md. Code Ann., Com. Law § 14-3503), and Maryland's Social Security Number Privacy Act (Md. Code Ann., Com. Law § 14-3401, *et seq*.);

e. Equifax engaged in unfair acts and practices by failing to disclose the data breach to Maryland Subclass members in a timely and accurate manner, in violation of Md. Code Ann., Com. Law § 14-3504(b)(3);

f. Equifax engaged in unfair acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Maryland Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

384. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

385. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Maryland Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maryland Subclass.

386. As a direct and proximate result of Defendant's unlawful practices, Maryland Subclass members suffered injury and/or damages.

387. Maryland Subclass members seek relief under Md. Code Ann., Com. Law § 13-408, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs.

S. Massachusetts

MASSACHUSETTS CONSUMER PROTECTION ACT
MASS. GEN. LAWS ANN. CH. 93A, § 1, *ET. SEQ.*
(BROUGHT BY THE MASSACHUSETTS-RESIDENT PLAINTIFF AND THE MASSACHUSETTS SUBCLASS)

388. Plaintiffs incorporate the above allegations by reference.

389. Plaintiff Scott Youngstrom is a resident of Massachusetts and was also a resident of Massachusetts when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Massachusetts Subclass.

390. On September 22, 2017, Plaintiff sent a demand for relief to Equifax, on behalf of the Massachusetts Subclass, prior to the filing of this complaint.

391. Equifax operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. ch. 93A, § 1.

392. Equifax engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of services in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a), in at least the following ways:

a. Equifax misrepresented material facts to Plaintiff and the Massachusetts Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Massachusetts Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to Plaintiff and the Massachusetts Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and the Massachusetts Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and the Massachusetts Subclass members' personal and financial information;

d. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiff and the Massachusetts Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, the Massachusetts Right of Privacy statute (Mass.

Gen. Laws Ann. ch. 214, § 1B), and the Massachusetts data breach statute (Mass. Gen. Laws Ann. ch. 93H, § 3(a));

e. Equifax engaged in unfair acts and practices by failing to disclose the data breach to Massachusetts Subclass members in a timely and accurate manner, in violation of Mass. Gen. Laws Ann. ch. 93H, § 3(a);

f. Equifax engaged in unfair acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Massachusetts Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

393. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within the penumbra of common law, statutory, or other established concepts of unfairness.

394. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Massachusetts Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Massachusetts Subclass.

395. As a direct and proximate result of Equifax's unlawful practices, Massachusetts Subclass members suffered injury and/or damages.

396. Massachusetts Subclass members seek relief under Mass. Gen. Laws Ann. ch. 93A, § 9, including, but not limited to, actual damages, statutory damages, double or treble damages, injunctive and/or other equitable relief, and/or attorneys' fees and costs.

T. Michigan

**MICHIGAN CONSUMER PROTECTION ACT
MICH. COMP. LAWS § 445.903, *ET SEQ.*
(BROUGHT BY THE MICHIGAN-RESIDENT
PLAINTIFF AND THE MICHIGAN SUBCLASS)**

397. Plaintiffs incorporate the above allegations by reference.

398. Plaintiff Robert Harris is a resident of Michigan and was also a resident of Michigan when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Michigan Subclass.

399. Plaintiff and Michigan Subclass members are "persons" within the meaning of MICH. COMP. LAWS § 445.902(1)(d).

400. The Michigan Consumer Protection Act ("Michigan CPA") prohibits "[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce …." MICH. COMP. LAWS § 445.903(1). Equifax engaged in unfair, unconscionable, or deceptive methods, acts or practices prohibited by the Michigan CPA, including: "(c) Representing that goods or services have … characteristics … that they do not have ….;" "(e) Representing that goods or services are of a particular standard … if they are of another;" "(i) Making false or misleading statements of fact concerning the reasons for, existence of, or amounts of price reductions;" "(s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;" "(bb) Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;" and "(cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner." MICH. COMP. LAWS § 445.903(1). By failing to disclose and actively concealing that its computer and data systems were not secure from hackers and thieves, that it had suffered multiple data breaches, and by

presenting itself as a reputable credit bureau that valued data security and stood behind consumers, Equifax engaged in deceptive business practices prohibited by the Michigan CPA.

401. In the course of its business, Equifax willfully failed to disclose and actively concealed its negligent data security, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its business.

402. Equifax knew it had failed to adequately protect consumers' data, and knew that its computer and data systems were not safe and secure, as advertised. Equifax knew this for at least several months, but concealed all of that information.

403. Equifax was also aware that it valued profits over data security, and that it was placing consumers' personal and financial information at risk of theft. Equifax concealed this information as well.

404. By failing to disclose that its computer and data systems were not safe and secure, by failing to disclose the data breaches that it suffered, and by presenting itself as a reputable credit bureau that valued data security and stood behind consumers, Equifax engaged in deceptive business practices in violation of the Michigan CPA.

405. In the course of Equifax's business, it willfully failed to disclose and actively concealed the risk posed by its inadequate data security measures. Equifax compounded the deception by failing to promptly disclose the numerous data breaches that it had suffered.

406. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the other Michigan Subclass members, about the true nature of its computer and data systems.

407. Equifax intentionally and knowingly misrepresented material facts regarding its computer and data security and data breaches with an intent to mislead Plaintiff and the Michigan Subclass.

408. Equifax knew or should have known that its conduct violated the Michigan CPA.

409. As alleged above, Equifax made material statements about the safety and security of its computer and data systems and the Equifax brand that were either false or misleading.

410. Equifax owed Plaintiff and Michigan Subclass members a duty to disclose the true nature of its computer and data security, and the devaluing of data security at Equifax, because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over data security, and that it was failing to notify consumers of its inadequate computer and data security and numerous data breaches;

b. Intentionally concealed the foregoing from Plaintiff and the Michigan Subclass; and/or

c. Made incomplete representations about the security of its computer and data systems generally, and that it had suffered numerous data breaches in particular, while purposefully withholding material facts from Plaintiff and the Michigan Subclass that contradicted these representations.

411. Equifax's fraudulent claims of high security and the true nature of its computer and data security were material to Plaintiff and the Michigan Subclass because the loss of personal and financial information to criminals can result in a

lifetime of lost time and expenses in connection with preventing and remediating harm from identity theft.

412. Plaintiff and the Michigan Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Class members would have taken important steps to protect their information from theft and misuse but for Equifax's violations of the Michigan CPA.

413. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Michigan CPA. All consumers whose personal and financial information was stolen suffered ascertainable loss in the form of out-of-pocket expenses to freeze credit accounts and protect against identity theft as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

414. Equifax's violations present a continuing risk to Plaintiff and the Michigan Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

415. As a direct and proximate result of Equifax's violations of the Michigan CPA, Plaintiff and the Michigan Subclass have suffered injury-in-fact and/or actual damage.

416. Plaintiff seeks injunctive relief to enjoin Equifax from continuing its unfair and deceptive acts; monetary relief against Equifax measured as the greater of (a) actual damages in an amount to be determined at trial and (b) statutory damages in the amount of $250 for Plaintiff and each Michigan Subclass member; reasonable attorneys' fees; and any other just and proper relief available under MICH. COMP. LAWS § 445.911.

417. Plaintiff and the Michigan Subclass also seeks punitive damages against Equifax because it carried out despicable conduct with willful and

conscious disregard of the rights and safety of others. Equifax intentionally and willfully misrepresented the security and reliability of its computer and data systems, concealed material facts that only they knew, and repeatedly promised Plaintiff and Michigan Subclass members that its computer and data systems were secure—all to avoid the expense and public relations nightmare of disclosing that its negligence resulted in the loss of the personal and financial information of 143 million Americans. Equifax's unlawful conduct constitutes malice, oppression, and fraud warranting punitive damages.

U. Minnesota

MINNESOTA CONSUMER FRAUD ACT
MINN. STAT. § 325F.68, ET. SEQ. AND MINN. STAT. § 8.31, ET. SEQ.
(BROUGHT BY THE MINNESOTA-RESIDENT PLAINTIFF AND THE MINNESOTA SUBCLASS)

418. Plaintiffs incorporate the above allegations by reference.

419. Plaintiff William Hill is a resident of Minnesota and was also a resident of Minnesota when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Minnesota Subclass.

420. Equifax engaged in unlawful practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of services in violation of Minn. Stat. Ann. § 325F.69, in at least the following ways:

a. Equifax misrepresented material facts to the Minnesota Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Minnesota Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to the Minnesota Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Minnesota Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Minnesota Subclass members' personal and financial information;

d. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Minnesota Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45); the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; and the Minnesota Unfair Claims Practices Act (Minn. Stat. § 72A.17, *et seq*.);

e. Equifax engaged in unlawful and deceptive acts and practices by failing to disclose the data breach to Minnesota Subclass members in a timely and accurate manner, in violation of Minn. Stat. Ann. § 325E.61(1)(a);

f. Equifax engaged in unlawful and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Minnesota Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

421. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

422. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Minnesota Subclass members'

personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Minnesota Subclass.

423. As a direct and proximate result of Defendant's unlawful practices, Minnesota Subclass members suffered injury and/or damages.

424. Minnesota Subclass members seek relief under Minn. Stat. Ann. § 8.31, including, but not limited to, damages, injunctive and/or other equitable relief, and attorneys' fees and costs.

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT MINN. STAT. § 325D.43, *ET. SEQ.* (BROUGHT BY THE MINNESOTA-RESIDENT PLAINTIFF AND THE MINNESOTA SUBCLASS)

425. Plaintiffs incorporate the above allegations by reference.

426. Plaintiff William Hill is a resident of Minnesota and was also a resident of Minnesota when the data breach occurred. He brings this Count on his own behalf and on behalf of members of the Minnesota Subclass.

427. Equifax engaged in deceptive practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation of Minn. Stat. § 325D.44, in at least the following ways:

a. Equifax misrepresented material facts to the Plaintiff and Minnesota Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Minnesota Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of Minn. Stat. § 325D.44(5), (7), (9), and (13);

b. Equifax misrepresented material facts to the Plaintiff and Minnesota Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Minnesota Subclass members' personal and financial information in violation of Minn. Stat. § 325D.44(5), (7), (9), and (13);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Minnesota Subclass members' personal and financial information in violation of Minn. Stat. § 325D.44(5), (7), (9), and (13);

d. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiff and Minnesota Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45); the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; and the Minnesota Unfair Claims Practices Act (Minn. Stat. § 72A.17, *et seq*.);

e. Equifax engaged in unlawful and deceptive acts and practices by failing to disclose the data breach to Plaintiff and Minnesota Subclass members in a timely and accurate manner, in violation of Minn. Stat. Ann. § 325E.61(1)(a);

f. Equifax engaged in unlawful and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Minnesota Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

428. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused

substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

429. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Minnesota Subclass members' personal and financial information, and that risk of a data breach or theft was highly likely. Defendant's actions in the above-described unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the members of the Minnesota Subclass.

430. As a direct and proximate result of Defendant's unlawful and deceptive trade practices, the data breach affected hundreds of thousands of Minnesotans. Even beyond these Minnesotans, the impact on the public is widespread, including the long-term impairment of credit scores, fraudulent tax filings, and national security implications.

431. As a direct and proximate result of Defendant's unlawful practices, Minnesota Subclass members suffered injury and/or damages.

432. Plaintiff and Minnesota Subclass members seek relief under Minn. Stat. § 325D.45, including, but not limited to, injunctive relief and attorneys' fees and costs, and also seek relief under Minn. Stat. Ann. § 8.31, including, but not limited to, damages.

V. Missouri

MISSOURI MERCHANDISING PRACTICES ACT
MO. REV. STAT. § 407.010, *ET SEQ*.
(BROUGHT BY THE MISSOURI-RESIDENT PLAINTIFF AND THE MISSOURI SUBCLASS)

433. Plaintiffs incorporate the above allegations by reference.

434. Plaintiff Chris Tinen is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

435. Plaintiff and Missouri Subclass members' personal and financial information was accessed and stored by the Defendant in connection with the purchase and sale of "merchandise" or services in "trade" or "commerce" as meant by Mo. Rev. Stat. § 407.010 .

436. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Mo. Rev. Stat. § 407.020(1), in at least the following ways:

a. Equifax misrepresented material facts to the Missouri Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Missouri Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to the Missouri Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Missouri Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Missouri Subclass members' personal and financial information;

d. Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Missouri Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act

(15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Missouri Unfair Trade Practice Act (Mo. Rev. Stat. § 375.936(4) and (6)(a));

e. Equifax engaged in unlawful and deceptive acts and practices by failing to disclose the data breach to Missouri Subclass members in a timely and accurate manner, in violation of Mo. Rev. Stat. § 407.1500(2)(1)(a);

f. Equifax engaged in unlawful and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Missouri Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

437. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

438. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Missouri Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Missouri Subclass.

439. As a direct and proximate result of Defendant's unlawful practices, Missouri Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

440. Missouri Subclass members seek relief under Mo. Rev. Stat. § 407.025, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

W. Nevada

NEVADA DECEPTIVE TRADE PRACTICES ACT NEV. REV. STAT. § 598.0915, *ET. SEQ.*; NEV. REV. STAT. § 41.600, *ET. SEQ.* (BROUGHT BY THE NEVADA-RESIDENT PLAINTIFF AND THE NEVADA SUBCLASS)

441. Plaintiffs incorporate the above allegations by reference.

442. Plaintiff Kenneth Peterson is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

443. In the course of its business, Equifax engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts, in at least the following ways:

a. Equifax misrepresented material facts to the Plaintiff and Nevada Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Nevada Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

b. Equifax misrepresented material facts to the Plaintiff and Nevada Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Nevada Subclass members' personal and financial information, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Nevada

Subclass members' personal and financial information, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

d. Equifax engaged in deceptive trade practices by failing to maintain the privacy and security of Plaintiff and Nevada Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, the Nevada Confidentiality and Disclosure of Information statute (Nev. Rev. Stat. § 695F.410), and the Nevada data breach statute (Nev. Rev. Stat. Ann. § 603A.210);

e. Equifax engaged in deceptive trade practices by failing to disclose the data breach to Nevada Subclass members in a timely and accurate manner, in violation of Nev. Rev. Stat. Ann. § 603A.220(1);

f. Equifax engaged in deceptive trade practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Nevada Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

444. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

445. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Nevada Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair

practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nevada Subclass.

446. As a direct and proximate result of Defendant's deceptive practices, Plaintiff and Nevada Subclass members suffered injury and/or damages.

447. Plaintiff and Nevada Subclass members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

X. New Hampshire

VIOLATION OF THE N.H. CONSUMER PROTECTION ACT N.H. REV. STAT. ANN. § 358A:1, *ET SEQ.* (BROUGHT BY THE NEW HAMPSHIRE-RESIDENT PLAINTIFF AND THE NEW HAMPSHIRE SUBCLASS)

448. Plaintiffs incorporate the above allegations by reference.

449. Plaintiff Walter Kivlan is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

450. The New Hampshire Consumer Protection Act ("CPA") prohibits a person, in the conduct of any trade or commerce, from engaging in "any unfair or deceptive act or practice in the conduct of any trade or commerce within this state." N.H. Rev. Stat. Ann. § 358-A:2.

451. Defendants are persons within the meaning of the CPA. *See* N.H. Rev. Stat. § 358A:1(I).

452. In the course of Defendant's business, Defendant failed to adequately protect and secure consumers' personal and financial date from hackers and thieves, and willfully failed to disclose and actively concealed its inadequate computer and data security as described above. Accordingly, Defendant engaged in unfair and unlawful acts.

453. Defendants' conduct was unfair because it offends established public policy, violates or offends state and federal statutory and common law, or falls within the penumbra of those laws, is immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers, including by violation of the state and federal privacy laws enumerated herein.

454. The computer and data security measures undertaken by Equifax were material to Plaintiff and the New Hampshire Subclass. Had Plaintiff and the New Hampshire Subclass known that their personal and financial information was at grave risk of theft, and was, in fact, stolen, they would have taken steps to protect themselves from identity theft and other losses.

455. Defendant's unfair and deceptive acts or practices, including its failure to disclose material information, has injured Plaintiff and the New Hampshire Subclass. Plaintiff and the New Hampshire Subclass have had to take timely and expensive steps to protect themselves from identity theft, including implementing and maintaining credit freezes and identity theft prevention measures.

456. Plaintiff and the New Hampshire Subclass are entitled to recover the greater of actual damages or $1,000 pursuant to N.H. Rev. Stat. § 358-A:10. Plaintiff and the New Hampshire Subclass are also entitled to treble damages because Defendant acted willfully in its unfair and deceptive practices.

Y. New Jersey

NEW JERSEY CONSUMER FRAUD ACT
N.J. STAT. ANN. § 56:8-1, *ET. SEQ.*
(BROUGHT BY THE NEW JERSEY-RESIDENT PLAINTIFF AND THE NEW JERSEY SUBCLASS)

457. Plaintiffs incorporate the above allegations by reference.

458. Plaintiff David Jungali is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

459. Defendant sells "merchandise," as meant by N.J. Stat. Ann. § 56:8-1, by products and services to the public, and by accessing and storing Plaintiff and New Jersey Subclass members' personal and financial information in connection with their purchase of merchandise from creditors or prospective creditors.

460. Equifax engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation of N.J. Stat. Ann. § 56:8-2, in at least the following ways:

a. Equifax misrepresented material facts to Plaintiff and the New Jersey Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and New Jersey Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to Plaintiff and the New Jersey Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and New Jersey Subclass members' personal and financial information;

c. Equifax knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and New Jersey Subclass members' personal and financial information with the intent that others rely on the omission, suppression, and concealment;

d. Equifax engaged in unconscionable and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and New Jersey Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax engaged in unconscionable and deceptive acts and practices by failing to disclose the data breach to Plaintiff and New Jersey Subclass members in a timely and accurate manner, in violation of N.J. Stat. Ann. § 56:8-163(a);

f. Equifax engaged in unconscionable and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and New Jersey Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

461. The above unlawful and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

462. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and New Jersey Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Jersey Subclass.

463. As a direct and proximate result of Defendant's unconscionable or deceptive acts and practices, Plaintiff and New Jersey Subclass members suffered an ascertainable loss in moneys or property, real or personal, as described above,

including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

464. Plaintiff and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

Z. New York

NEW YORK GENERAL BUSINESS LAW
N.Y. GEN. BUS. LAW § 349, *ET. SEQ.*
(BROUGHT THE NEW YORK-RESIDENT PLAINTIFF AND THE NEW YORK SUBCLASS)

465. Plaintiffs incorporate the above allegations by reference.

466. Plaintiff Patricia Buhler is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

467. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), in at least the following ways:

a. Equifax misrepresented and fraudulently advertised material facts to Plaintiff and the New York Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and New York Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to Plaintiff and the New York Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and New York Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for Plaintiff and New York Subclass members' personal and financial information;

d. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff and New York Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Plaintiff and New York Subclass members in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2);

f. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and New York Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

468. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and New York Subclass members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information, and the loss of the benefit of their bargain.

469. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

470. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and New York Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New York Subclass.

471. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

AA. North Carolina

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT N.C. GEN. STAT. ANN. § 75-1.1, *ET. SEQ.* (BROUGHT BY THE NORTH CAROLINA-RESIDENT PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

472. Plaintiffs incorporate the above allegations by reference.

473. Plaintiffs Emily Bosak and Sean Bosak are residents of the above state and were also residents of such state when the data breach occurred. Plaintiffs bring this Count on Plaintiffs' own behalf and on behalf of members of the above state Subclass.

474. Defendant's conduct and omissions affected commerce, as meant by N.C. Gen. Stat. § 75-1.1.

475. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation of N.C. Gen. Stat. § 75-1.1 in at least the following ways:

a. Equifax misrepresented material facts to Plaintiffs and the North Carolina Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs and North Carolina Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to Plaintiffs and the North Carolina Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs and North Carolina Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiffs and North Carolina Subclass members' personal and financial information;

d. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiffs and North Carolina Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, the North Carolina Consumer and Customer Information Privacy Act (N.C. Gen. Stat. § 58-39-1, *et seq*.), and the North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. § 5863-15(1) and (2));

e. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to disclose the data breach to Plaintiffs and North Carolina Subclass members in a timely and accurate manner, in violation of N.C. Gen. Stat. Ann. § 7665(a);

f. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiffs and North Carolina Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

476. The above unfair, unlawful, and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

477. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs and North Carolina Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Carolina Subclass.

478. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive acts and practices, Plaintiffs and North Subclass members suffered injury and/or damages.

479. Plaintiffs and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 75-16.1 including, but not limited to, injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

BB. North Dakota

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT
N.D. CENT. CODE § 51-10-01, *ET. SEQ.*
(BROUGHT BY THE NORTH DAKOTA-RESIDENT PLAINTIFF AND THE NORTH DAKOTA SUBCLASS)

480. Plaintiffs incorporate the above allegations by reference.

481. Plaintiff Justin Peltier is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

482. Defendant sells and advertises "merchandise," as meant by N.D. Cent. Code § 51-1501, and it accessed and stored the Plaintiff and North Dakota Subclass members' personal and financial information in connection with the purchase and sale of merchandise from prospective creditors or creditors.

483. Equifax engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation of N.D. Cent. Code § 51-15-01 in at least the following ways:

a. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Plaintiff and North Dakota Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and North Dakota Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to Plaintiff and the North Dakota Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and North Dakota Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and North Dakota Subclass members' personal and financial information, with the intent that others rely on the omission, suppression, and concealment;

d. Equifax engaged in deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and North Dakota Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule; the North Dakota Privacy of Consumer Financial and Health Information rule (N.D. Admin. Code 45-14-01-01, *et seq*.);

e. Equifax engaged in deceptive acts and practices by failing to disclose the data breach to Plaintiff and North Dakota Subclass members in a timely and accurate manner, in violation of N.D. Cent. Code Ann. § 51-30-02;

f. Equifax engaged in deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and North Dakota Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

484. The above deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

485. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and North Dakota Subclass members' personal and financial information and that risk of a data

breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Dakota Class.

486. As a direct and proximate result of Defendant's deceptive acts and practices, Defendant acquired money or property from Plaintiff and North Dakota Subclass members.

487. Plaintiff and North Carolina Subclass members seek relief under N.D. Cent. Code Ann. § 51-15-09 including, but not limited to, injunctive relief, damages, restitution, treble damages, and attorneys' fees and costs.

CC. Ohio

VIOLATION OF OHIO CONSUMER SALES PRACTICES ACT
OHIO REV. CODE ANN. § 1345, *ET SEQ.*
(BROUGHT BY THE OHIO-RESIDENT PLAINTIFF AND THE OHIO SUBCLASS)

488. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

489. Plaintiff Peter Maizitis is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

490. Equifax's conduct constitutes unfair or deceptive acts or practices in connection with a consumer transaction with the meaning of the Ohio Consumers Sales Practices Act, Ohio Rev. Code Ann. § 1345, *et. seq.*

491. As a result of Equifax's unfair or deceptive acts or practices in connection with a consumer transaction, Plaintiff and Ohio Subclass members suffered injury in fact and lost property and money.

492. Equifax's misrepresentations and omissions were material to Plaintiff and Ohio Subclass members' transactions with Equifax and were made knowingly and with reason to know that Plaintiff and Ohio Subclass members would rely on the misrepresentations and omissions.

493. Plaintiff and Ohio Subclass members reasonably relied on Equifax's misrepresentations and omissions and suffered harm as a result. Plaintiff and Ohio Subclass members were injured in fact by: damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) the general nuisance and annoyance of dealing with all these issues resulting from the Equifax data breach; and (e) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

494. Plaintiff and Ohio Subclass members seek restitution, injunctive relief and statutory damages, to the extent permitted by applicable law,on behalf of the Class.

495. Equifax conducted the practices alleged herein in the course of its business, pursuant to standardized practices that it engaged in both before and after the Plaintiff and Ohio Subclass members in this case were harmed, these acts have been repeated millions of times, and many consumers were affected.

DD. Oklahoma

OKLAHOMA CONSUMER PROTECTION ACT
OKLA. STAT. ANN. TIT. 15, § 751, *ET. SEQ.*
(BROUGHT BY THE OKLAHOMA-RESIDENT PLAINTIFF AND THE OKLAHOMA SUBCLASS)

496. Plaintiffs incorporate the above allegations by reference.

497. Plaintiff Jerry Nutt is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

498. Plaintiff and the Oklahoma Subclass members purchased "merchandise," as meant by Okla. Stat. tit. 15, § 752, from prospective creditors and creditors who sent or accessed their personal and financial information via the Defendant, which also accessed and stored it.

499. Plaintiff and the Oklahoma Subclass members' interactions with the Defendant, or the transactions which led to the Defendant accessing and storing their personal and financial information, constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752.

500. Equifax engaged in unlawful, unfair, and deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by Plaintiff and the Oklahoma Subclass in violation of Okla. Stat. tit. 15, § 753, in at least the following ways:

a. Equifax knowingly, or with reason to know, misrepresented material facts to Plaintiff and the Oklahoma Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Oklahoma Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of Okla. Stat. tit. 15, § 753(5) and (8);

b. Equifax knowingly, or with reason to know, misrepresented material facts to Plaintiff and the Oklahoma Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Oklahoma Subclass members' personal and financial information in violation of Okla. Stat. tit. 15, § 753(5) and (8);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Oklahoma Subclass members' personal and financial information in violation of Okla. Stat. tit. 15, § 753(5) and (8);

d. Equifax engaged in unfair, unlawful, and deceptive trade practices by failing to maintain the privacy and security of Plaintiff and Oklahoma Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Oklahoma Privacy of Consumer Financial and Health Information regulation (Okla. Admin. Code §§ 365:35-1-40, 365:35-1-20);

e. Equifax engaged in unlawful, unfair, and deceptive trade practices by failing to disclose the data breach to Plaintiff and Oklahoma Subclass members in a timely and accurate manner, in violation of Okla. Stat. Ann. Tit 24, § 163(A);

f. Equifax engaged in unlawful, unfair, and deceptive trade practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Oklahoma Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

501. The above unlawful, unfair, and deceptive trade practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused

substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

502. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Oklahoma Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Oklahoma Subclass.

503. As a direct and proximate result of Defendant's deceptive acts and practices, the Oklahoma Subclass members suffered injury and/or damages.

504. Plaintiff and Oklahoma Subclass members seek relief under Okla. Stat. Ann. tit. 15, § 761.1 including, but not limited to, injunctive relief, actual damages, statutory damages, and attorneys' fees and costs.

EE. Oregon

OREGON UNLAWFUL TRADE PRACTICES ACT OR. REV. STAT. §§ 646.605, *ET SEQ.* (BROUGHT BY THE OREGON-RESIDENT PLAINTIFF AND THE OREGON SUBCLASS)

505. Plaintiffs incorporate the above allegations by reference.

506. Plaintiff Marie Chinander is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

507. Equifax is a person within the meaning of OR. REV. STAT. § 646.605(4)

508. Purchases made by Plaintiff and Oregon Subclass members for which Equifax provided credit bureau services are "goods" obtained primarily for

personal family or household purposes within the meaning of OR. REV. STAT. § 646.605(6).

509. The Oregon Unfair Trade Practices Act ("Oregon UTPA") prohibits a person from, in the course of the person's business, doing any of the following: "(e) Represent[ing] that … goods … have … characteristics … uses, benefits, … or qualities that they do not have; (g) Represent[ing] that … goods … are of a particular standard [or] quality … if they are of another; (i) Advertis[ing] … goods or services with intent not to provide them as advertised;" and "(u) engag[ing] in any other unfair or deceptive conduct in trade or commerce." OR. REV. STAT. § 646.608(1).

510. Equifax engaged in unlawful trade practices, including representing that its computer and data systems have characteristics, uses, benefits, and qualities which they do not have; representing that its computer and data security is of a particular standard and quality when they are not; and engaging in other unfair or deceptive acts.

511. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its provision of credit bureau services and identity theft prevention services.

512. Equifax's actions as set forth above occurred in the conduct of trade or commerce.

513. Equifax knew it had inadequate computer and data security and that consumers' personal and financial information was at risk. Equifax knew this for at least several months, but concealed all of that information.

514. Equifax was also aware that it valued profits over the security of consumers' data, and that it was collecting and warehousing millions of

consumers' personal and financial information in computer and data systems that did not have the security and integrity advertised and jeopardized the security of consumers' personal and financial information. Equifax concealed this information as well.

515. By failing to disclose that its computer and data systems were inadequately secured, by failing to disclose its numerous data breaches, and by presenting itself as a reputable credit bureau that valued the personal and financial information of consumers and stood behind consumers, Equifax engaged in deceptive business practices in violation of the Oregon UTPA.

516. In the course of Equifax's business, it willfully failed to disclose and actively concealed the risk posed by its lack of adequate computer and data security. Equifax compounded the deception by failing to disclose its numerous data breaches.

517. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and Oregon Subclass members, about the true security of its computer and data systems, the quality of the Equifax brand, and the devaluing of consumers' personal and financial information at Equifax.

518. Equifax intentionally and knowingly misrepresented material facts regarding its credit bureau services with an intent to mislead Plaintiff and the Oregon Subclass.

519. Equifax knew or should have known that its conduct violated the Oregon UTPA.

520. As alleged above, Equifax made material statements about the security and integrity of its computer and data systems and the Equifax brand that were either false or misleading.

521. Equifax owed Plaintiff and the Oregon Subclass a duty to disclose the true nature of its computer and data security, and the devaluing of consumers' personal and financial information at Equifax, because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over data security and integrity;

b. Intentionally concealed the foregoing from Plaintiff and the Oregon Subclass; and/or

c. Made incomplete representations about the security and integrity of its computer and data systems generally, and the data breaches it suffered in particular, while purposefully withholding material facts from Plaintiff and the Oregon Subclass that contradicted these representations.

522. Equifax's fraudulent claims of data and computer security and the true nature of its systems were material to Plaintiff and the Oregon Subclass.

523. Plaintiff and the Oregon Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Plaintiff and the Oregon Subclass members who knew of Equifax's inadequate security measures would have taken steps to prevent the theft of their personal and financial information and would have also taken steps to protect their personal and financial information from use by thieves and criminals.

524. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Oregon UTPA. Plaintiff and the Oregon Subclass members suffered ascertainable loss in the form of out-of-pocket expenses and time associated with implementing and maintaining credit freezes and identity theft prevention measures, as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

525. Equifax's violations present a continuing risk to Plaintiff and the Oregon Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

526. As a direct and proximate result of Equifax's violations of the Oregon UTPA, Plaintiff and the Oregon Subclass have suffered injury-in-fact and/or actual damage.

527. Plaintiff and the Oregon Subclass are entitled to recover the greater of actual damages or $200 pursuant to OR. REV. STAT. § 646.638(1). Plaintiff and the Oregon Subclass are also entitled to punitive damages because Equifax engaged in conduct amounting to a particularly aggravated, deliberate disregard of the rights of others.

FF. Pennsylvania

PENNSYLVANIA UNFAIR TRADE PRACTICES 73 PA CONS. STAT. ANN. § 201-1, *ET. SEQ.* (BROUGHT BY THE PENNSYLVANIA-RESIDENT PLAINTIFF AND THE PENNSYLVANIA SUBCLASS)

528. Plaintiffs incorporate the above allegations by reference.

529. Plaintiff Raymond McCartney is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

530. Plaintiff and the Pennsylvania Subclass members' personal and financial information was accessed and stored by the Defendant in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2, for personal, family, and/or household purposes, *i.e.*, in connection with those members' consumer transactions for those personal, family, and/or household purposes.

531. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material

facts with respect to the sale and advertisement of the services purchased by Plaintiff and the Pennsylvania Subclass in violation of 73 Pa. Cons. Stat. § 201-3, in at least the following ways:

a. Equifax misrepresented material facts to the Pennsylvania Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Pennsylvania Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of 73 Pa. Cons. Stat. § 201-3(4)(v), (ix), and (xxi);

b. Equifax misrepresented material facts to the Pennsylvania Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Pennsylvania Subclass members' personal and financial information in violation of 73 Pa. Cons. Stat. § 201-3(4)(v), (ix), and (xxi);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Pennsylvania Subclass members' personal and financial information in violation of in violation of 73 Pa. Cons. Stat. § 201-3(4)(v), (ix), and (xxi);

d. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and Pennsylvania Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to disclose the data breach to Plaintiff and Pennsylvania

Subclass members in a timely and accurate manner, in violation of 73 Pa. Cons. Stat. § 2303(a);

f. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Pennsylvania Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

532. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

533. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Pennsylvania Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Pennsylvania Subclass.

534. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and the Pennsylvania Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

535. Plaintiff and Pennsylvania Subclass members seek relief under 73 Pa. Cons. Stat. § 201-9.2, including, but not limited to, injunctive relief, actual damages or $100 per Class member, whichever is greater, treble damages, and attorneys' fees and costs.

GG. Rhode Island

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT
R.I. GEN. LAWS § 6-13.1, *ET. SEQ.*
(BROUGHT BY THE RHODE ISLAND-RESIDENT PLAINTIFF AND THE RHODE ISLAND SUBCLASS)

536. Plaintiffs incorporate the above allegations by reference.

537. Plaintiff Patricia Maggiacomo is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

538. The Rhode Island Subclass members purchased goods and services in "trade" and "commerce," as meant by R.I. Gen. Laws § 6-13.1-1, for personal, family, and/or household purposes, from prospective creditors and creditors who accessed and shared their personal and financial information with the Defendant, which in turn accessed and stored it in "trade" and "commerce."

539. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by Plaintiff and the Rhode Island Subclass in violation of R.I. Gen. Laws Ann. § 6-13.1-2, in at least the following ways:

a. Equifax misrepresented material facts to Plaintiff and the Rhode Island Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Rhode Island Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of R.I. Gen. Laws Ann. § 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);

b. Equifax misrepresented material facts to Plaintiff and the Rhode Island Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Rhode Island Subclass members' personal and financial information in violation of R.I. Gen. Laws Ann. § 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Rhode Island Subclass members' personal and financial information in violation of in violation of R.I. Gen. Laws Ann. § 6-13.1-1(6)(v), (vii), (ix), (xii), (xiii), and (xiv);

d. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and Rhode Island Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Rhode Island data breach statute (R.I. Gen. Laws § 11-49.2-2(2));

e. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to disclose the data breach to Plaintiff and Rhode Island Subclass members in a timely and accurate manner, in violation of R.I. Gen. Laws Ann. § 11-49.2-3(a);

f. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Rhode Island Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

540. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused

substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

541. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Rhode Island Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Rhode Island Subclass.

542. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and the Rhode Island Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

543. Plaintiff and Rhode Island Subclass members seek relief under R.I. Gen. Laws § 6-13.1-5.2, including, but not limited to, injunctive relief, other equitable relief, actual damages or $200 per Class member, whichever is greater, punitive damages, and attorneys' fees and costs.

HH. South Carolina

VIOLATIONS OF THE SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT S.C. CODE ANN. § 39-5-10, ET SEQ. (BROUGHT BY THE SOUTH CAROLINA-RESIDENT PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

544. Plaintiffs incorporate the above allegations by reference.

545. Plaintiff Michael Moore is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

546. Defendant is a "person" under S.C. CODE ANN. § 39-5-10.

547. The South Carolina Unfair Trade Practices Act ("South Carolina UTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce . . . ." S.C. CODE ANN. § 39-5-20(a). Equifax's actions as set herein occurred in the conduct of trade or commerce.

548. In the course of its business, Equifax willfully failed to disclose and actively concealed its inadequate computer and data security, that it had suffered numerous data breaches, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its provision of credit bureau services.

549. Equifax knew it had taken inadequate measures to ensure the security and integrity of its computer and data systems and it knew it had suffered numerous data breaches. Equifax knew this for at least several months, but concealed all of that information.

550. Equifax was also aware that it valued profits over the security of consumers' personal and financial information, and that it had suffered numerous data breaches. Equifax concealed this information as well.

551. By failing to disclose that its computer and data security measures were inadequate, that it had suffered numerous data breaches, and by presenting itself as a reputable credit bureau that valued consumers' personal and financial information and stood behind consumers, Equifax engaged in deceptive business practices in violation of the South Carolina UTPA.

552. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and South Carolina

Subclass members, about the inadequacy of Equifax's computer and data security and the quality of the Equifax brand.

553. Equifax intentionally and knowingly misrepresented material facts regarding the security and integrity of its computer and data systems with an intent to mislead Plaintiff and the South Carolina Subclass.

554. Equifax knew or should have known that its conduct violated the South Carolina UTPA.

555. As alleged above, Equifax made material statements about the security and integrity of its computer and data systems and the Equifax brand that were either false or misleading.

556. Equifax owed Plaintiff and the South Carolina Subclass a duty to disclose the true nature of its computer and data systems, and the devaluing of data security at Equifax, because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over the security of consumers' data;

b. Intentionally concealed the foregoing from Plaintiff and the South Carolina Subclass; and/or

c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its prior data breaches in particular, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

557. Equifax's fraudulent claims of data and computer security and the true nature of its computer and data system security were material to Plaintiff and the South Carolina Subclass.

558. Plaintiff and the South Carolina Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Plaintiff and South Carolina Subclass members;

personal and financial information would not have been stolen but for Equifax's violations of the South Carolina UTPA.

559. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the South Carolina UTPA. Plaintiff and the South Carolina Subclass members suffered ascertainable loss in the form of the theft of their personal and financial information as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

560. Equifax's violations present a continuing risk to Plaintiff and the South Carolina Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

561. As a direct and proximate result of Equifax's violations of the South Carolina UTPA, Plaintiffs and the South Carolina Subclass have suffered injury-in-fact and/or actual damage.

562. Pursuant to S.C. CODE ANN. § 39-5-140(a), Plaintiff and the South Carolina Subclass seek monetary relief against Equifax to recover for their economic losses. Because Equifax's actions were willful and knowing, Plaintiff and the South Carolina Subclass members' damages should be trebled. *Id.*

563. Plaintiff and the South Carolina Subclass further allege that Equifax's malicious and deliberate conduct warrants an assessment of punitive damages because Equifax carried out despicable conduct with willful and conscious disregard of the rights and safety of others, subjecting Plaintiff and the South Carolina Subclass to cruel and unjust hardship as a result. Equifax's intentionally and willfully misrepresented the security and integrity of their computer and data systems, deceived Plaintiff and the South Carolina Subclass and concealed material facts that only Equifax knew. Equifax's unlawful conduct constitutes malice, oppression, and fraud warranting punitive damages.

564. Plaintiff and the South Carolina Subclass further seek an order enjoining Equifax's unfair or deceptive acts or practices.

II. South Dakota

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT S.D. CODIFIED LAWS § 37-24-1, *ET. SEQ.* (BROUGHT BY THE SOUTH DAKOTA-RESIDENT PLAINTIFF AND THE SOUTH DAKOTA SUBCLASS)

565. Plaintiffs incorporate the above allegations by reference.

566. Plaintiff David Steufen is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

567. Defendant advertises and sells "goods or services" and/or "merchandise" in "trade" and "commerce," as meant by S.D. Codified Laws § 37-24-1.

568. Equifax engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation of S.D. Codified Laws § 37-24-6, in at least the following ways:

a. Equifax knowingly and intentionally misrepresented material facts to Plaintiff and the South Dakota Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and South Dakota Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of S.D. Codified Laws § 37-24-6(1);

b. Equifax knowingly and intentionally misrepresented material facts to Plaintiff and the South Dakota Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and South Dakota Subclass members' personal and financial information in violation of S.D. Codified Laws § 37-24-6(1);

c. Equifax knowingly and intentionally omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and South Dakota Subclass members' personal and financial information in violation of in violation of S.D. Codified Laws § 37-24-6(1);

d. Equifax engaged in deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and South Dakota Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax knowingly and intentionally engaged in deceptive acts and practices by failing to disclose the data breach to Plaintiff and South Dakota Subclass members in a timely and accurate manner;

f. Equifax engaged in deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and South Dakota Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

569. The above deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

570. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and South Dakota Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the South Dakota Class.

571. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and the South Dakota Subclass members were adversely affected, injured, and/or damaged.

572. Plaintiff and South Dakota Subclass members seek relief under S.D. Codified Laws § 37-24-31, including, but not limited to, actual damages.

JJ. Tennessee

TENNESSEE CONSUMER PROTECTION ACT TENN. CODE ANN. §§ 47-18-101, *ET. SEQ.* (BROUGHT BY THE TENNESSEE-RESIDENT PLAINTIFF AND THE TENNESSEE SUBCLASS)

573. Plaintiffs incorporate the above allegations by reference.

574. Plaintiff Jeannie Baggett is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

575. Defendant advertised and sold "goods" or "services" in "trade" and "commerce," as meant by Tenn. Code Ann. § 47-18-103.

576. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation Tenn. Code Ann. § 47-18-104, in at least the following ways:

a. Equifax misrepresented material facts to Plaintiff and the Tennessee Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Tennessee Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

b. Equifax misrepresented material facts to Plaintiff and the Tennessee Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Tennessee Subclass members' personal and financial information in violation of Tenn. Code Ann. § 4718-104(b)(5) and (9);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Tennessee Subclass members' personal and financial information in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

d. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and Tennessee Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Tennessee Unfair Trade Practices and Unfair Claims Settlement Act of 2009 (Tenn. Code Ann. § 56-8-104(1)(A) and (2));

e. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to disclose the data breach to Plaintiff and Tennessee Subclass members in a timely and accurate manner, in violation of Tenn. Code Ann. § 47-18-2107(b);

f. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Tennessee Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

577. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

578. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Tennessee Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Tennessee Subclass.

579. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and the Tennessee Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

580. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. § 47-18-109, including, but not limited to, injunctive relief, actual damages, treble damages for each willful or knowing violation, and attorneys' fees and costs.

KK. Texas

TEXAS DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT TEX. BUS. & COM. CODE § 17.41, *ET. SEQ.* (BROUGHT BY THE TEXAS-RESIDENT PLAINTIFF AND THE TEXAS SUBCLASS)

581. Plaintiffs incorporate the above allegations by reference.

582. Plaintiff Cheryl Lawson is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

583. Plaintiffs sent a demand for relief to Equifax on behalf of the Texas Subclass on September 22, 2017.

584. Plaintiffs and Texas Subclass members are consumers, as defined in Tex. Bus. & Com. Code § 17.45(4).

585. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Tex. Bus. & Com. Code § 17.46, in at least the following ways:

a. Equifax misrepresented and fraudulently advertised material facts to the Texas Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Texas Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft, in violation of Tex. Bus. & Com. Code § 17.46(b)(5), (7), (9), and (24);

b. Equifax misrepresented material facts to Plaintiff and the Texas Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Texas Subclass members' personal and financial information in violation of Tex. Bus. & Com. Code § 17.46(b)(5), (7), (9), and (24);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Texas Subclass members' personal and financial information, in violation of Tex. Bus. & Com. Code § 17.46(b)(5), (7), (9), and (24) and §17.50(d);

d. Equifax engaged in unconscionable trade acts or practices in violation of Tex. Bus. & Com. Code § 17.50(a)(3) and §17.50(d) failing to maintain the privacy and security of Plaintiff and Texas Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Texas data breach statute (Tex. Bus. & Com. Code Ann. § 521.052(a);

e. Equifax engaged in unconscionable trade acts or practices in violation of Tex. Bus. & Com. Code § 17.50(a)(3) and § 17.50(d) by failing to disclose the data breach to Plaintiff and Texas Subclass members in a timely and accurate manner, contrary to the duties imposed by Tex. Bus. & Com. Code Ann. § 521.053(b);

f. Equifax engaged in unconscionable trade acts or practices in violation of Tex. Bus. & Com. Code § 17.50(a)(3) and §17.50(d) by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Texas Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

586. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Texas Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their

legally protected interest in the confidentiality and privacy of their personal and financial information.

587. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

588. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Texas Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Texas Subclass.

589. Plaintiff and Texas Subclass members seek relief under Tex. Bus. & Com. Code § 17.50, including, but not limited to, economic damages, damages for mental anguish, treble damages, injunctive relief, restitution, and attorneys' fees and costs.

LL. Utah

UTAH CONSUMER SALES PRACTICES ACT
UTAH CODE ANN. § 13-11-1, ET SEQ.
(BROUGHT BY THE UTAH-RESIDENT PLAINTIFF AND THE UTAH SUBCLASS)

590. Plaintiffs incorporate the above allegations by reference.

591. Plaintiff Ivy Madsen is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

592. The Utah Consumer Sales Practices Act ("Utah CSPA") makes unlawful any "deceptive act or practice by a supplier in connection with a consumer transaction" under UTAH CODE ANN. § 13-11-4. Specifically, "a supplier

commits a deceptive act or practice if the supplier knowingly or intentionally: (a) indicates that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not" or "(b) indicates that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not." UTAH CODE ANN. § 13-11-4. "An unconscionable act or practice by a supplier in connection with a consumer transaction" also violates the Utah CSPA. UTAH CODE ANN. § 13-11-5.

593. In the course of its business, Equifax willfully failed to disclose and actively concealed its inadequate computer and data security discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with the provision of credit bureau services in Utah.

594. Equifax knew it had inadequate computer and data security, and knew that it had suffered numerous data breaches. Equifax knew this for several months, but concealed all of that information.

595. Equifax was also aware that it valued profits over the security of consumers' personal and financial information, and that it was inadequately protecting the personal and financial information of hundreds of millions of consumers. Equifax concealed this information as well.

596. By failing to disclose that its computer and data systems were not secure, that it had suffered numerous data breaches and by presenting itself as a reputable credit bureau that valued consumers' personal and financial information and stood behind consumers, Equifax engaged in deceptive business practices in violation of the Utah CSPA.

597. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the Utah Subclass members, about the true nature of its computer and data systems and the quality of the Equifax brand.

598. Equifax intentionally and knowingly misrepresented material facts regarding its computer and data systems with an intent to mislead Plaintiff and the Utah Subclass.

599. Equifax knew or should have known that its conduct violated the Utah CSPA.

600. Equifax owed Plaintiff a duty to disclose the true nature of its computer and data systems, and the devaluing of consumers' information at Equifax, because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over computer and data security, and that it had suffered numerous data breaches;

b. Intentionally concealed the foregoing from Plaintiff and the Utah Subclass; and/or

c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its numerous data breaches in particular, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

601. Equifax's fraudulent claims of computer and data security and the true nature of such systems were material to Plaintiff and the Utah Subclass.

602. Plaintiff and the Utah Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Class members would have taken steps to prevent the loss of their personal and financial information, and would not have had their information stolen from Equifax but for Equifax's violations of the Utah CSPA.

603. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Utah CSPA. Plaintiff and the Utah Subclass members suffered ascertainable loss in the form of the out-of-pocket expenses for credit freezes and identity theft monitoring as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

604. Equifax's violations present a continuing risk to Plaintiff and the Utah Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

605. As a direct and proximate result of Equifax's violations of the Utah CSPA, Plaintiff and the Utah Subclass have suffered injury-in-fact and/or actual damage.

606. Pursuant to UTAH CODE ANN. § 13-11-4, Plaintiff and the Utah Subclass seek monetary relief against Equifax measured as the greater of (a) actual damages in an amount to be determined at trial and (b) statutory damages in the amount of $2,000 for each Plaintiff and each Utah Subclass member, reasonable attorneys' fees, and any other just and proper relief available under the Utah CSPA.

MM. Vermont

VERMONT CONSUMER FRAUD ACT
VT. STAT. ANN. TIT. 9, § 2451, *ET. SEQ.*
(BROUGHT BY THE VERMONT-RESIDENT PLAINTIFF AND THE VERMONT SUBCLASS)

607. Plaintiffs incorporate the above allegations by reference.

608. Plaintiff Scott Kingsland is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

609. Plaintiff and the Vermont Subclass members are "consumers" as meant by Vt. Stat. Ann. tit. 9, § 2451a.

610. Plaintiff and the Vermont Subclass members purchased "goods" or "services," as meant by Vt. Stat. Ann. tit. 9, § 2451a., from prospective creditors and creditors who accessed or shared their personal and financial information with the Defendant, which in turn accessed and stored it.

611. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in violation of Vt. Stat. Ann. tit. 9, § 2453, in at least the following ways:

a. Equifax misrepresented material facts to the Vermont Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Vermont Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to the Vermont Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Vermont Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Vermont Subclass members' personal and financial information;

d. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and Vermont Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to disclose the data breach to Plaintiff and Vermont Subclass members in a timely and accurate manner, in violation of Vt. Stat. Ann. tit. 9, § 2435(b)(1);

f. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Vermont Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

612. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

613. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Vermont Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Vermont Subclass.

614. As a direct and proximate result of Defendant's deceptive acts and practices, the Vermont Subclass members suffered injury and/or damages.

615. Plaintiff and Vermont Subclass members seek relief under Vt. Stat. Ann. tit. 9, § 2461, including, but not limited to, injunctive relief, restitution, actual damages, disgorgement of profits, exemplary damages, and attorneys' fees and costs.

NN. Virginia

VIRGINIA CONSUMER PROTECTION ACT
VA. CODE ANN. §§ 59.1-196, *ET SEQ.*
(BROUGHT BY THE VIRGINIA-RESIDENT PLAINTIFF AND THE VIRGINIA SUBCLASS)

616. Plaintiffs incorporate the above allegations by reference.

617. Plaintiff Georgeann Roberts is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

618. The Virginia Consumer Protection Act ("Virginia CPA") prohibits "…(5) misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits; (6) misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; … (8) advertising goods or services with intent not to sell them as advertised …; [and] (14) using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction[.]" VA. CODE ANN. § 59.1-200(A).

619. Defendant is a "person" as defined by VA. CODE ANN. § 59.1-198. The transactions between Plaintiff and the Virginia Subclass members on one hand and Equifax on the other, leading to the purchase or lease of products or the taking of loans or opening of accounts, are "consumer transactions" as defined by VA. CODE ANN. § 59.1-198.

620. In the course of Equifax's business, it willfully failed to disclose and actively concealed its inadequate computer and data security. Accordingly, Equifax engaged in acts and practices violating VA. CODE ANN. § 59.1-200(A), including representing that its computer and data systems have characteristics, uses, benefits, and qualities which they do not have; representing that its computer

and data security is of a particular standard and quality when they are not and otherwise engaging in conduct likely to deceive.

621. In the course of its business, Equifax willfully failed to disclose and actively concealed its deficient security measures discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with the provision of credit bureau services.

622. Equifax knew it had inadequate computer and data security, and knew that it had suffered numerous data breaches. Equifax knew this for at least several months, but concealed all of that information.

623. Equifax was also aware that it valued profits over the security of consumers' personal and financial information. Equifax concealed this information as well.

624. By failing to disclose that its computer and data security were inadequate, that it had suffered numerous data breaches, and by presenting itself as a reputable credit bureau that valued consumers' personal and financial information and stood behind consumers, Equifax engaged in deceptive business practices in violation of the Virginia CPA.

625. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the Virginia Subclass members, about the true nature of its computer and data security, the quality of the Equifax brand, and the devaluing of consumers' information at Equifax.

626. Equifax intentionally and knowingly misrepresented material facts regarding its computer and data security with an intent to mislead Plaintiff and the Virginia Subclass.

627. Equifax knew or should have known that its conduct violated the Virginia CPA.

628. As alleged above, Equifax made material statements about the security and integrity of its computer and data systems and the Equifax brand that were either false or misleading.

629. Equifax owed Plaintiff and the Virginia Subclass a duty to disclose the true nature of the security of its computer and data systems, and the devaluing of security of consumer information at Equifax, because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over security of consumers' information;

b. Intentionally concealed the foregoing from Plaintiff and the Virginia Subclass; and/or

c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its numerous data breaches in particular, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

630. Equifax's fraudulent claims of computer and data security and the true nature of its security were material to Plaintiff and the Virginia Subclass.

631. Plaintiff and the Virginia Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Plaintiff and the Virginia Subclass would have taken steps to prevent the theft of their personal and financial information and would have taken steps to prevent the use of their information by criminals but for Equifax's violations of the Virginia CPA.

632. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Virginia CPA. Plaintiff and the Virginia Subclass members suffered ascertainable loss in the form of out of pocket expenses

for credit freezes and identity theft monitoring as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

633. Equifax's violations present a continuing risk to Plaintiff and the Virginia Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

634. As a direct and proximate result of Equifax's violations of the Virginia CPA, Plaintiff and the Virginia Subclass have suffered injury-in-fact and/or actual damage.

635. Plaintiff and the Virginia Subclass members were injured as a result of Equifax's conduct. These injuries are the direct and natural consequence of Equifax's misrepresentations and omissions.

636. Equifax actively and willfully concealed and/or suppressed the material facts regarding its computer and data security with the intent to deceive and mislead Plaintiff and the Virginia Subclass. Plaintiff and the Virginia Subclass members therefore seek treble damages.

OO. Washington

WASHINGTON CONSUMER PROTECTION ACT
WASH. REV. CODE § 19.86.020, *ET. SEQ.*
(BROUGHT BY THE WASHINGTON-RESIDENT PLAINTIFF AND THE WASHINGTON SUBCLASS)

637. Plaintiffs incorporate the above allegations by reference.

638. Plaintiff Peter de Jesus is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

639. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020, in at least the following ways:

a. Equifax misrepresented and fraudulently advertised material facts to Plaintiff and the Washington Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Washington Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts to Plaintiff and the Washington Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Washington Subclass members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Washington Subclass members' personal and financial information;

d. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff and Washington Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, and the Washington regulations pertaining to Privacy of Consumer Financial and Health Information (Wash. Admin. Code § 284-04-300);

e. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Plaintiff and Washington Subclass members in a timely and accurate manner, contrary to the duties imposed by Wash. Rev. Code § 19.255.010(1);

f. Equifax engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and Washington Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

640. As a direct and proximate result of Defendant's deceptive trade practices, Washington Subclass members suffered injury and/or damages.

641. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

642. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Washington Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Washington Subclass.

643. Plaintiff and Washington Subclass members seek relief under Wash. Rev. Code § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

PP. West Virginia

WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT
W. VA. CODE § 46A-6-101, *ET. SEQ.*
(BROUGHT BY THE WEST VIRGINIA-RESIDENT PLAINTIFF AND THE WEST VIRGINIA SUBCLASS)

644. Plaintiffs incorporate the above allegations by reference.

645. Plaintiff Tanya Palmer is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

646. Plaintiff sent a demand for relief to Equifax on behalf of the West Virginia Subclass prior to the filing of this complaint.

647. Plaintiff and the West Virginia Subclass relied on Equifax's services in "trade" or "commerce," as meant by W. Va. Code Ann. § 46A-6-102, for personal, family, and/or household purposes.

648. Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by Plaintiff and the West Virginia Subclass in violation of W. Va. Code Ann. § 46A-6-104, in at least the following ways:

a. Equifax misrepresented material facts pertaining to the security practices and procedures necessary to safeguard Plaintiff and West Virginia Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft in violation of W. Va. Code Ann. § 46A-6-102(7)(E), (I), (L), (M), and (N);

b. Equifax misrepresented material facts to Plaintiff and the West Virginia Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and West Virginia Subclass members' personal and financial information in violation of W. Va. Code Ann. § 46A-6-102(7)(E), (I), (L), (M), and (N);

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and West

Virginia Subclass members' personal and financial information in violation of W. Va. Code Ann. § 46A-6-102(7)(E), (I), (L), (M), and (N);

d. Equifax engaged in unfair, unlawful, and deceptive acts and practices by failing to maintain the privacy and security of Plaintiff and West Virginia Subclass members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule;

e. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to disclose the data breach to Plaintiff and West Virginia Subclass members in a timely and accurate manner, in violation of W.V. Code § 46A-2A-102(a);

f. Equifax engaged in unlawful, unfair, and deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff and West Virginia Subclass members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

649. The above unlawful, unfair, and deceptive acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

650. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and West Virginia Subclass members' personal and financial information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or

wanton and reckless with respect to the rights of members of the West Virginia Subclass.

651. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and the West Virginia Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal and financial information.

652. Plaintiff and West Virginia Subclass members seek relief under W. Va. Code § 46A-6-106 and 46A-5104, including, but not limited to, injunctive relief, actual damages or $200, whichever is greater, and attorneys' fees and costs.

QQ. Wisconsin

WISCONSIN DECEPTIVE TRADE PRACTICES ACT WIS. STAT. § 110.18 (BROUGHT BY THE WISCONSIN-RESIDENT PLAINTIFF AND THE WISCONSIN SUBCLASS)

653. Plaintiffs incorporate the above allegations by reference.

654. Plaintiff Zandra Mendoza is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

655. Equifax is a "person, firm, corporation or association" within the meaning of WIS. STAT. § 100.18(1).

656. Plaintiff and Wisconsin Subclass Members are members of "the public" within the meaning of WIS. STAT. § 100.18(1).

657. The Wisconsin Deceptive Trade Practices Act ("Wisconsin DTPA") prohibits a "representation or statement of fact which is untrue, deceptive or misleading." WIS. STAT. § 100.18(1).

658. In the course of its business, Equifax willfully failed to disclose and actively concealed its inadequate computer and data security discussed herein and

otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its provision of credit bureau services.

659. Equifax knew it had inadequate computer and data security and knew that it had suffered numerous data breaches. Equifax knew this for at least several months, but concealed all of that information.

660. Equifax was also aware that it valued profits over the security of consumers' personal and financial information. Equifax concealed this information as well.

661. By failing to disclose that its computer and data systems were inadequately secured, that it had suffered numerous data breaches, and by presenting itself as a reputable credit bureau that valued consumers' personal and financial information and stood behind consumers, Equifax engaged in deceptive business practices in violation of the Wisconsin DTPA.

662. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and Wisconsin Subclass members, about the true nature of its computer and data security and the quality of the Equifax brand.

663. Equifax intentionally and knowingly misrepresented material facts regarding the security and integrity of its computer and data systems with an intent to mislead Plaintiff and the Wisconsin Subclass.

664. Equifax knew or should have known that its conduct violated the Wisconsin DTPA.

665. As alleged above, Equifax made material statements about the security and integrity of its computer and data systems, and the Equifax brand that were either false or misleading.

666. Equifax owed Plaintiff and the Wisconsin Subclass a duty to disclose the true nature of the security of its computer and data systems, because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over the security of consumers' information, and that it had suffered numerous data breaches;

b. Intentionally concealed the foregoing from Plaintiff and the Wisconsin Subclass; and/or

c. Made incomplete representations about the security and integrity of its computer and data systems generally, and its numerous prior data breaches in particular, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

667. Equifax's fraudulent claims of computer and data security and the true nature of the security of such systems were material to Plaintiff and the Wisconsin Subclass.

668. Plaintiff and the Wisconsin Subclass suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information. Class members would not have had their personal and financial information stolen and would have taken steps to prevent identity theft and other harms, but for Equifax's violations of the Wisconsin DTPA.

669. Equifax had an ongoing duty to all Equifax customers to refrain from unfair and deceptive practices under the Wisconsin DTPA. All Subclass members suffered ascertainable loss in the form of out of pocket expenses and lost time to implement and maintain credit freezes and identity theft prevention as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

670. Equifax's violations present a continuing risk to Plaintiff and the Wisconsin Subclass as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

671. As a direct and proximate result of Equifax's violations of the Wisconsin DTPA, Plaintiff and the Wisconsin Subclass have suffered injury-in-fact and/or actual damage.

672. Plaintiff and the Wisconsin Subclass are entitled to damages and other relief provided for under WIS. STAT. § 100.18(11)(b)(2). Because Equifax's conduct was committed knowingly and/or intentionally, Plaintiff and the Wisconsin Subclass are entitled to treble damages.

673. Plaintiff and the Wisconsin Subclass also seek court costs and attorneys' fees under WIS. STAT. § 110.18(11)(b)(2).

COUNT V
DATA BREACH STATUTES
(BROUGHT BY THE STATE-RESIDENT PLAINTIFFS AND THE STATE SUBCLASSES BELOW)

A. California

VIOLATION OF CALIFORNIA DATA BREACH ACT
CAL. CIV. CODE § 1798.80, *ET SEQ.*
(BROUGHT BY THE CALIFORNIA-RESIDENT PLAINTIFF AND THE CALIFORNIA SUBCLASS)

674. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

675. Plaintiffs Deborah Person and Amanda Chap are residents of the above state and were also residents of such state when the data breach occurred. Plaintiffs bring this Count on Plaintiffs' own behalf and on behalf of members of the above state Subclass.

676. Section 1798.82 of the CALIFORNIA CIVIL CODE provides, in pertinent part, as follows:

(a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

* * *

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

677. The data breach constituted a “breach of the security system” of Equifax.

678. Plaintiffs and California Subclass members’ names, addresses, emails, birthdates, Social Security numbers, employment and income information constitute “personal information.”

679. Equifax unreasonably delayed in informing anyone about the breach of security of Plaintiffs and California Subclass members’ confidential and non-public information after Equifax knew the data breach had occurred.

680. Equifax failed to disclose to Plaintiffs and California Subclass members without unreasonable delay and in the most expedient time possible, the breach of security of consumers’ personal and financial information when they knew or reasonably believed such information had been compromised.

681. Upon information and belief, no law enforcement agency instructed Equifax that notification to Plaintiffs and California Subclass members would impede investigation.

682. Pursuant to Section 1798.84 of the CALIFORNIA CIVIL CODE:

(a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

* * *

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

683. Plaintiffs, individually and on behalf of the California Subclass, seek all remedies available under CAL. CIV. CODE § 1798.84, including, but not limited to: (a) damages suffered by Plaintiffs and California Subclass members as alleged above; (b) statutory damages for Equifax's willful, intentional, and/or reckless violation of CAL. CIV. CODE § 1798.83; and (c) equitable relief.

684. Plaintiffs, on behalf of themselves and the California Subclass, also seek reasonable attorneys' fees and costs under CAL. CIV. CODE § 1798.84(g).

B. Colorado

**COLO. REV. STAT. ANN. § 6-1-716(2), *ET. SEQ*.
(BROUGHT BY THE COLORADO-RESIDENT PLAINTIFF AND THE COLORADO SUBCLASS)**

685. Plaintiffs incorporate the above allegations by reference.

686. Plaintiff Timothy Hutz is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

687. Equifax is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security system in the

most expedient time possible and without unreasonable delay under Colo. Rev. Stat. Ann. § 6-1716(2).

688. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Colo. Rev. Stat. Ann. § 6-1-716(1),(2).

689. Plaintiff and Colorado Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered by Colo. Rev. Stat. Ann. § 6-1-716(1),(2).

690. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. Ann. § 6-1-716 (2).

691. Thus, by failing to disclose the data breach in a timely and accurate manner, Equifax violated Colo. Rev. Stat. Ann. § 6-1-716 (2).

692. As a direct and proximate result of Equifax's violations of Colo. Rev. Stat. Ann. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

693. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. Ann. § 6-1-716(4), including, but not limited to, actual damages and equitable relief.

C. Georgia

GA. CODE ANN. § 10-1-912(A), *ET. SEQ.*
(BROUGHT BY THE GEORGIA-RESIDENT PLAINTIFF AND THE GEORGIA SUBCLASS)

694. Plaintiffs incorporate the above allegations by reference.

695. Plaintiff Dawn Evans is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

696. Equifax is required to accurately notify Plaintiff and Georgia Subclass members if it becomes aware of a breach of its data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Georgia Subclass members' personal and financial information) in the most expedient time possible and without unreasonable delay under Ga. Code Ann. § 10-1-912(a).

697. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Ga. Code Ann. § 10-1-912(a).

698. Plaintiff and Georgia Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Ga. Code Ann. § 10-1-912(a).

699. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Georgia Subclass members' personal and financial information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

700. Thus, by failing to disclose the data breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a).

701. As a direct and proximate result of Equifax's violations of Ga. Code Ann. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

702. Plaintiff and Georgia Subclass members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

D. Hawaii

HAW. REV. STAT. § 487N-2(A), *ET. SEQ.* (BROUGHT BY THE HAWAII-RESIDENT PLAINTIFF AND THE HAWAII SUBCLASS)

703. Plaintiffs incorporate the above allegations by reference.

704. Plaintiff Jennifer Griffin is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

705. Equifax is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

706. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Haw. Rev. Stat. § 487N-2(a).

707. Plaintiff and Hawaii Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Haw. Rev. Stat. § 487N-2(a).

708. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

709. Thus, by failing to disclose the data breach in a timely and accurate manner, Equifax violated Haw. Rev. Stat. § 487N-2(a).

710. As a direct and proximate result of Equifax's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages, as described above.

711. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including, but not limited to, actual damages.

E. Illinois

VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT AND CONSUMER FRAUD ACT (ON BEHALF OF ILLINOIS-RESIDENT PLAINTIFF AND THE ILLINOIS SUBCLASS)

712. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

713. Plaintiff Scott Sroka is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

714. The Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/1, provides that any data collector that owns or licenses personal information concerning a state resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.

715. Equifax is a "data collector" within the meaning of the IPIPA, 815 ILCS 530/5.

716. Equifax possessed Plaintiff and Illinois Subclass members' "personal information" within the meaning of the IPIPA, 815 ILCS 530/5.

717. The compromise of Plaintiff and Illinois Subclass members' personal and financial information constitutes a "breach of the security of the system data" or "breach" within the meaning of the IPIPA, 815 ILCS 530/5.

718. Under 815 ILCS 530/10(a) Equifax is required after a beach to notify Illinois residents "in the most expedient time possible and without unreasonable delay[.]"

719. Equifax had a duty to disclose in the most expedient time possible and without unreasonable delay that a breach of Plaintiff and Illinois Subclass members' personal information occurred.

720. Equifax failed to disclose in the most expedient time possible and without unreasonable delay that Plaintiff and Illinois Subclass members' personal and financial information was compromised.

721. At this time it is unknown whether the cost to provide individual notice to each Illinois resident who was affected by the breach exceeds $500,000.

722. Equifax's notice of the data breach was made only on its corporate website and does not comport with the Act's conspicuous posting requirement for notice of a breach.

723. Equifax violated Illinois law by delaying disclosure until six weeks after it was first notified of (or learned of) the breach.

724. A violation of Section 20 of the IPIPA constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1.

725. Equifax's conduct complained of was inexcusable and reckless indifference towards the rights of others.

726. Plaintiff and Illinois Subclass members were injured by Equifax's failure to properly implement adequate, commercially reasonable security measures to protect their personal and financial information that Equifax kept and used in its business.

727. Equifax's conduct constituted unfair and/or deceptive acts and practices, in violation of 815 ILCS 505/2, by:

a. Failing to properly implement adequate, commercially reasonable security measures to protect its customers' personal and financial information. Such actions for failing to maintain proper data security can be enforced by the FTC under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). *E.g. Federal Trade Commission v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHXPRG (D. Ariz.);

b. Failing to warn consumers that their information was at risk as a result of Equifax's failure to properly implement such measures; and

c. Failing to immediately notify affected consumers of the nature and extent of the security breach.

F. Iowa

IOWA CODE ANN. § 715C.2(1), *ET. SEQ.* (BROUGHT BY THE IOWA-RESIDENT PLAINTIFF AND THE IOWA SUBCLASS)

728. Plaintiffs incorporate the above allegations by reference.

729. Plaintiff Patricia Tuel is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

730. Equifax is required to accurately notify Plaintiff and Iowa Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code Ann. § 715C.2(1).

731. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Iowa Code Ann. § 715C.2(1).

732. Plaintiff and Iowa Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Iowa Code Ann. § 715C.2(1).

733. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code Ann. § 715C.2(1).

734. Thus, by failing to disclose the data breach in a timely and accurate manner, Equifax violated Iowa Code Ann. § 715C.2(1).

735. As a direct and proximate result of Equifax's violations of Iowa Code Ann. § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as above.

736. Plaintiff and Iowa Subclass members seek relief under Iowa Code Ann. § 714.16(7), including, but not limited to, actual damages and injunctive relief.

G. Louisiana

LA. REV. STAT. ANN. ANN. § 51:3074(A), *ET. SEQ.*
(BROUGHT BY THE LOUISIANA-RESIDENT PLAINTIFF AND THE LOUISIANA SUBCLASS)

737. Plaintiffs incorporate the above allegations by reference.

738. Plaintiff Randi Freeman is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

739. Equifax is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Louisiana Subclass members' personal and financial information) in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. Ann. § 51:3074(C).

740. Defendant is a business that owns or licenses computerized data that includes personal information as defined by La. Rev. Stat. Ann. Ann. § 51:3074(C).

741. Plaintiff and Louisiana Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under La. Rev. Stat. Ann. Ann. § 51:3074(C).

742. Because Equifax was aware of a breach of its security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Louisiana Subclass members' personal and financial information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. Ann. § 51:3074(C).

743. As a direct and proximate result of Equifax' violations of La. Rev. Stat. Ann. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

744. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. Ann. § 51:3075, including, but not limited to, actual damages.

H. Michigan

MICH. COMP. LAWS ANN. § 445.72(1), *ET. SEQ.* (BROUGHT BY THE MICHIGAN-RESIDENT PLAINTIFF AND THE MICHIGAN SUBCLASS)

745. Plaintiffs incorporate the above allegations by reference.

746. Plaintiff Robert Harris is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

747. Equifax is required to accurately notify Plaintiff and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted personal and financial information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

748. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

749. Plaintiff and Michigan Subclass members' personal and financial information (e.g. Social Security numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

750. Because Equifax discovered a security breach and had notice of a security breach (where unencrypted and unredacted personal and financial information was accessed or acquired by unauthorized persons), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

751. As a direct and proximate result of Equifax's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages, as above.

752. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including, but not limited to, a civil fine.

I. New Hampshire

N.H. REV. STAT. ANN. § 359-C:20(I)(A), *ET. SEQ.*
(BROUGHT BY THE NEW HAMPSHIRE-RESIDENT PLAINTIFF AND THE NEW HAMPSHIRE SUBCLASS)

753. Plaintiffs incorporate the above allegations by reference.

754. Plaintiff Walter Kivlan is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

755. Equifax is required to accurately notify Plaintiff and New Hampshire Subclass members if Equifax becomes aware of a breach of its data security system (in which misuse of personal and financial information has occurred or is reasonably likely to occur) as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

756. Defendant is a business that owns or licenses computerized data that includes personal information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

757. Plaintiff and New Hampshire Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

758. Because Equifax was aware of a security breach (in which misuse of personal and financial information has occurred or is reasonably likely to occur), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

759. As a direct and proximate result of Equifax's violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages, as described above.

760. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including, but not limited to, actual damages and injunctive relief.

J. Oregon

OR. REV. STAT. ANN. § 646A.604(1), *ET. SEQ.*
(BROUGHT BY THE OREGON-RESIDENT PLAINTIFF AND THE OREGON SUBCLASS)

761. Plaintiffs incorporate the above allegations by reference.

762. Plaintiff Marie Chinander is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

763. Pursuant to Or. Rev. Stat. Ann. § 646A.622(1), a business "that maintains records which contain personal information" of a Oregon resident "shall implement and maintain reasonable security measures to protect those records

from unauthorized access, acquisition, destruction, use, modification or disclosure."

764. Defendant is a business that maintains records which contain personal information, within the meaning of Or. Rev. Stat. Ann. § 646A.622(1), about Plaintiff and Oregon Subclass members.

765. Defendant violated Or. Rev. Stat. Ann. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff and Oregon Subclass members' personal and financial information,

766. Equifax is required to accurately notify Plaintiff and Oregon Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. Ann. § 646A.604(1).

767. Defendant is a business that owns, maintains, or otherwise possesses data that includes consumers personal information as defined by Or. Rev. Stat. Ann. § 646A.604(1).

768. Plaintiff and Oregon Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Or. Rev. Stat. Ann. § 646A.604(1).

769. Because Equifax discovered a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. Ann. § 646A.604(1).

770. As a direct and proximate result of Defendant's violations of Or. Rev. Stat. Ann. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass members suffered damages, as described above.

771. Plaintiff and Oregon Subclass members seek relief under Or. Rev. Stat. § 646A.624(3), including, but not limited to, actual damages and injunctive relief.

K. South Carolina

S.C. CODE ANN. § 39-1-90(A), *ET. SEQ.*
(BROUGHT BY THE SOUTH CAROLINA-RESIDENT PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

772. Plaintiffs incorporate the above allegations by reference.

773. Plaintiff Michael Moore is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

774. Equifax is required to accurately notify Plaintiff and South Carolina Subclass members following discovery or notification of a breach of its data security system (if personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm) in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

775. Defendant is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

776. Plaintiff and South Carolina Subclass members' personal and financial information (e.g., Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

777. Because Equifax discovered a breach of its data security system (in which personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

778. As a direct and proximate result of Equifax's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass members suffered damages, as described above.

779. Plaintiff and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including, but not limited to, actual damages and injunctive relief.

L. Tennessee

TENN. CODE ANN. § 47-18-2107(B), *ET. SEQ.* (BROUGHT BY THE TENNESSEE-RESIDENT PLAINTIFF AND THE TENNESSEE SUBCLASS)

780. Plaintiffs incorporate the above allegations by reference.

781. Plaintiff Jeannie Baggett is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

782. Equifax is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security system (in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person) in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

783. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

784. Plaintiff and Tennessee Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

785. Because Equifax discovered a breach of its security system (in which unencrypted personal information was, or is reasonably believed to have been,

acquired by an unauthorized person), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

786. As a direct and proximate result of Equifax' violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

787. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), 47-18-2104(f), including, but not limited to, actual damages, injunctive relief and treble damages.

M. Virginia

VA. CODE ANN. § 18.2-186.6(B), *ET. SEQ.*
(BROUGHT BY THE VIRGINIA-RESIDENT PLAINTIFF AND THE VIRGINIA SUBCLASS)

788. Plaintiffs incorporate the above allegations by reference.

789. Plaintiff Georgeann Roberts is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

790. Equifax is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of its data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

791. Defendant are entities that owns or licenses computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

792. Plaintiff and Virginia Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

793. Because Equifax discovered a breach of its security system (in which unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

794. As a direct and proximate result of Equifax's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

795. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, actual damages.

N. Washington

WASH. REV. CODE ANN. § 19.255.010(1), *ET. SEQ.* (BROUGHT BY THE WASHINGTON-RESIDENT PLAINTIFF AND THE WASHINGTON SUBCLASS)

796. Plaintiffs incorporate the above allegations by reference.

797. Plaintiff Peter de Jesus is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

798. Equifax is required to accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of its data security system (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not

secured) in the most expedient time possible and without unreasonable delay under Wash. Rev. Code Ann. § 19.255.010(1).

799. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.010(1).

800. Plaintiff and Washington Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.010(5).

801. Because Equifax discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1).

802. As a direct and proximate result of Equifax' violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiff and Washington Subclass members suffered damages, as described above.

803. Plaintiff and Washington Subclass members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(10)(a), 19.255.010(10)(b) including, but not limited to, actual damages and injunctive relief.

O. Wisconsin

WIS. STAT. ANN. § 134.98(2), *ET. SEQ.*
(BROUGHT BY THE WISCONSIN-RESIDENT PLAINTIFF AND THE WISCONSIN SUBCLASS)

804. Plaintiffs incorporate the above allegations by reference.

805. Plaintiff Zandra Mendoza is a resident of the above state and was also a resident of such state when the data breach occurred. Plaintiff brings this Count on Plaintiff's own behalf and on behalf of members of the above state Subclass.

806. Equifax is required to accurately notify Plaintiff and Wisconsin Subclass members if it knows that personal information in its possession has been acquired by a person whom it has not authorized to acquire the personal information within a reasonable time under Wis. Stat. Ann. §§ 134.98(2)-(3)(a).

807. Defendant is a business that maintains or licenses personal information as defined by Wis. Stat. Ann. § 134.98(2).

808. Plaintiff and Wisconsin Subclass members' personal and financial information (e.g., Social Security numbers) includes personal information as covered under Wis. Stat. Ann. § 134.98(1)(b).

809. Because Equifax knew that personal information in its possession had been acquired by a person whom it has not authorized to acquire the personal information, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. Ann. § 134.98(2).

810. As a direct and proximate result of Equifax' violations of Wis. Stat. Ann. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

811. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. Ann. § 134.98, including, but not limited to, actual damages and injunctive relief.

812. Equifax's actions described herein show willful misconduct, malice, fraud, wantonness, oppression, or that entire want of care which raises the presumption of conscious indifference to consequences. Further, Equifax acted and/or failed to act with the specific intent to cause harm to Plaintiffs. As a result, Plaintiffs are entitled to an award of punitive damages under O.C.G.A. Section 51-12-5.1.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiffs to be Class and/or Subclass representatives and their counsel to be Class Counsel;

B. That the Court award Plaintiffs and the Class and/or Subclasses appropriate relief, to include actual and statutory damages, disgorgement, and restitution, and punitive, including under O.C.G.A. § 51-12-5.1, exemplary, or multiple damages where available;

C. That the Court award Plaintiffs and the Class and/or Subclasses preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

D. Such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations; and

E. That the Court award Plaintiffs and the Class and/or Subclasses such other, favorable relief as may be available and appropriate under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully submitted, this 22nd day of September, 2017.

ROBBINS GELLER RUDMAN & DOWD LLP

By *_/s/ John C. Herman_*
John C. Herman,
(Ga. Bar No. 348370)
Monarch Centre, Suite 1650
3424 Peachtree Road, N.E.
Atlanta, GA 30326
Telephone: (404) 504-6500
Facsimile: (404) 504-6501
jherman@rgrdlaw.com

Thomas E. Loeser (*pro hac vice* to be filed)
Robert F. Lopez (*pro hac vice* to be filed)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
toml@hbsslaw.com
robl@hbsslaw.com

Paul J. Geller (*pro hac vice* to be filed)
Stuart A. Davidson (*pro hac vice* to be filed)
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: (561) 750-3000
Facsimile: (561) 750-3364
pgeller@rgrdlaw.com
sdavidson@rgrdlaw.com

Attorneys for Plaintiffs and the Proposed Classes